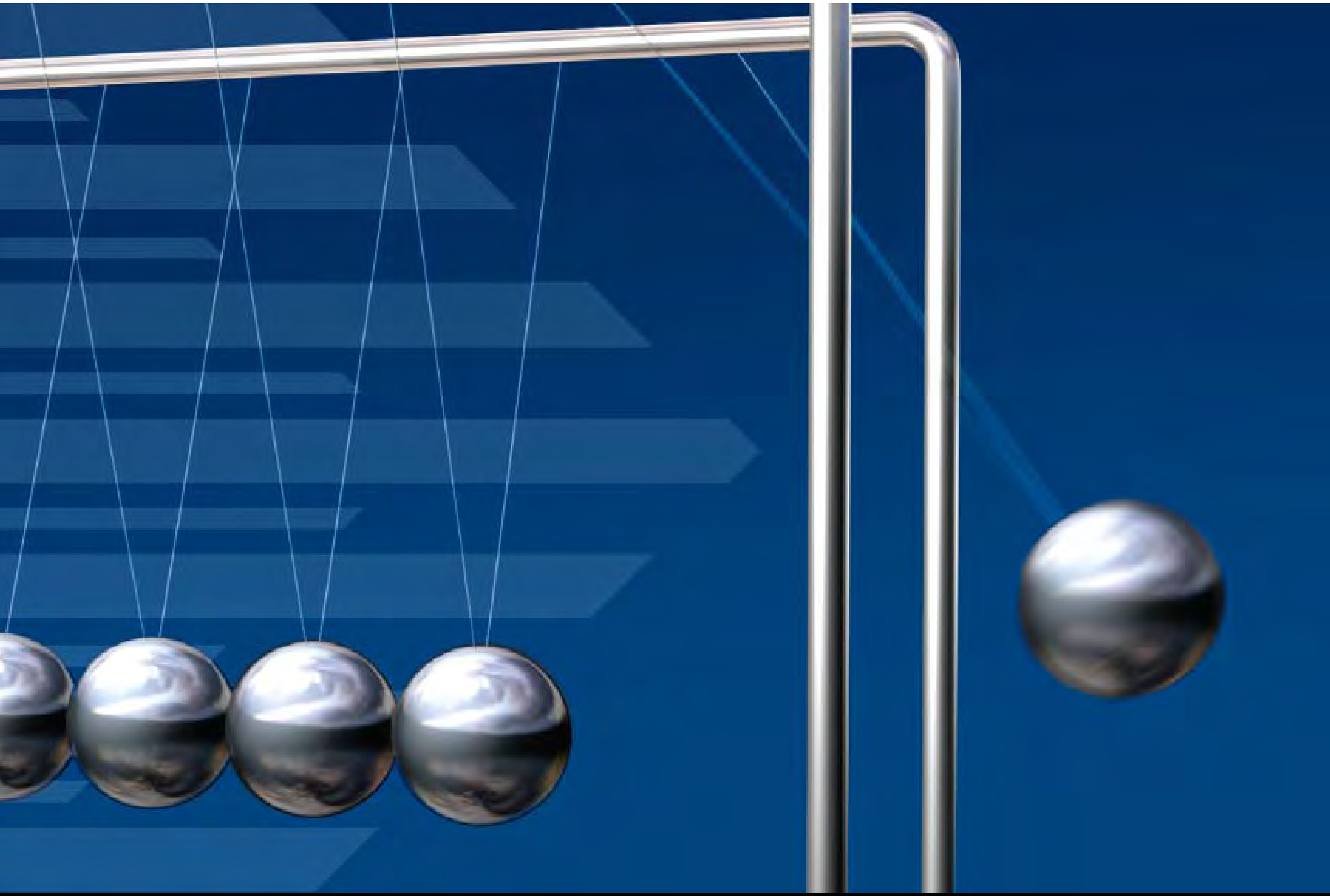


Year in Review 2008

Software Engineering Institute | Carnegie Mellon

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **2008**	2. REPORT TYPE	3. DATES COVERED **00-00-2008 to 00-00-2008**

4. TITLE AND SUBTITLE **Year in Review 2008**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University,Software Engineering Institute,Pittsburgh,PA,15213**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR’S ACRONYM(S)
	11. SPONSOR/MONITOR’S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**48**	

Contents

CARNEGIE MELLON UNIVERSITY
SOFTWARE ENGINEERING INSTITUTE

A Message from the Director

Software is Essential, Everywhere, and Expanding

The impact of software in our lives continues to grow. The men and women of the SEI have a deep knowledge and understanding of today's software problems and opportunities. They play a crucial role in advancing the state of the practice in ways that have a positive impact, certainly for our customers, but also for the industries they participate in and the world at large.

The SEI's women and men perform innovative research and interact with the global software community to find best practices and important new research, but most importantly, work hard to effectively transition technology, techniques, and methods to our clients and stakeholders. We teach individuals about architecture, security, interoperability, the integration of systems, and process improvement across the entire development life cycle. We conduct workshops for software educators, and through our Virtual Training Environment (VTE), we enable customers to have anywhere, anytime access to some of the best software training. Through our SEI Webinar and CERT Podcast series, we are engaging in Web 2.0 technologies to reach new audiences. And through direct support of government and industry clients, we improve the acquisition and development of software-intensive systems.

This Year in Review highlights a few ways the SEI creates customer solutions across a spectrum of challenges in areas ranging from digital forensics and process management to acquisition and architecture. Current examples highlighted in this issue include:

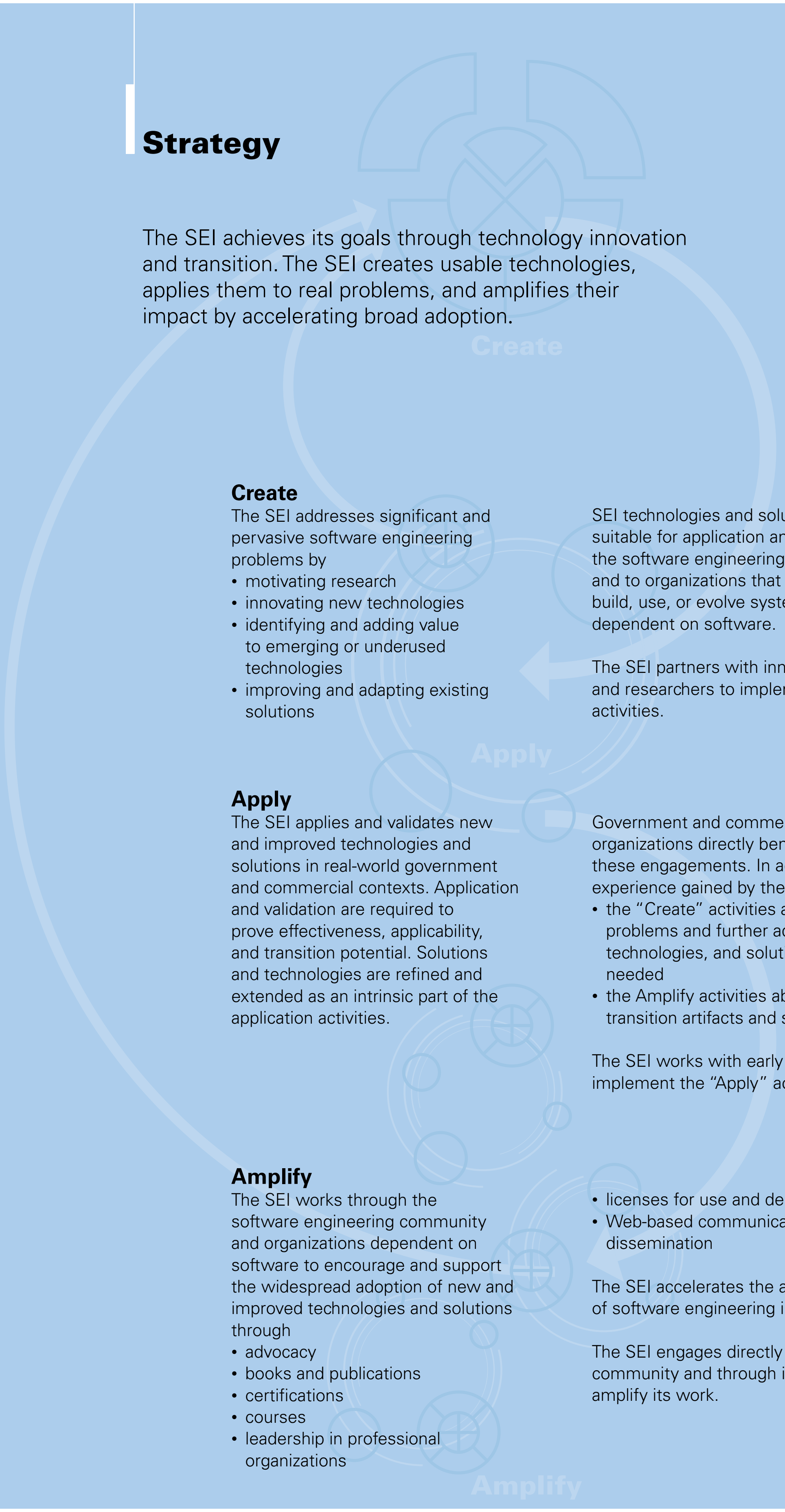
- Collaborations with the Army Strategic Software Improvement Program (ASSIP) to establish a stronger, more efficient, and more capable software community within the Army
- Creation of a comprehensive new set of tools and methods in computer forensics to help law enforcement capture crucial digital evidence for some high-profile cases
- Adoption of SEI's Team Software Process (TSP) methodology by the Mexican government in its work to build a national reputation as a provider of IT products and services
- Recognition by the Aerospace Vehicle Systems Institute (AVSI) of the SEI-developed Architecture Analysis and Design Language (AADL) as the ideal tool to help plan and build next-generation aerospace systems

I am proud to share some of our 2008 accomplishments and future research endeavors. These achievements are the result of an outstanding and dedicated staff working with a set of world-class customers. The United States has made a strong and committed investment in the development of technology, and the SEI is proud to serve as a global leader in the creation of knowledge and promotion of software engineering.

Paul D. Nielsen, Director and CEO

Strategy

The SEI achieves its goals through technology innovation and transition. The SEI creates usable technologies, applies them to real problems, and amplifies their impact by accelerating broad adoption.



Create

The SEI addresses significant and pervasive software engineering problems by

- motivating research
- innovating new technologies
- identifying and adding value to emerging or underused technologies
- improving and adapting existing solutions

SEI technologies and solutions are suitable for application and transition to the software engineering community and to organizations that commission, build, use, or evolve systems that are dependent on software.

The SEI partners with innovators and researchers to implement these activities.

Apply

The SEI applies and validates new and improved technologies and solutions in real-world government and commercial contexts. Application and validation are required to prove effectiveness, applicability, and transition potential. Solutions and technologies are refined and extended as an intrinsic part of the application activities.

Government and commercial organizations directly benefit from these engagements. In addition, the experience gained by the SEI informs

- the "Create" activities about real-world problems and further adjustments, technologies, and solutions that are needed
- the Amplify activities about needed transition artifacts and strategies

The SEI works with early adopters to implement the "Apply" activities.

Amplify

The SEI works through the software engineering community and organizations dependent on software to encourage and support the widespread adoption of new and improved technologies and solutions through

- advocacy
- books and publications
- certifications
- courses
- leadership in professional organizations
- licenses for use and delivery
- Web-based communication and dissemination

The SEI accelerates the adoption and impact of software engineering improvements.

The SEI engages directly with the community and through its partners to amplify its work.

Areas of Work

The SEI technical program—created and carried out by world-recognized leaders in software engineering, security, and process management—consists of four technical focus areas. The SEI also conducts new research into emerging topics in software and systems engineering.

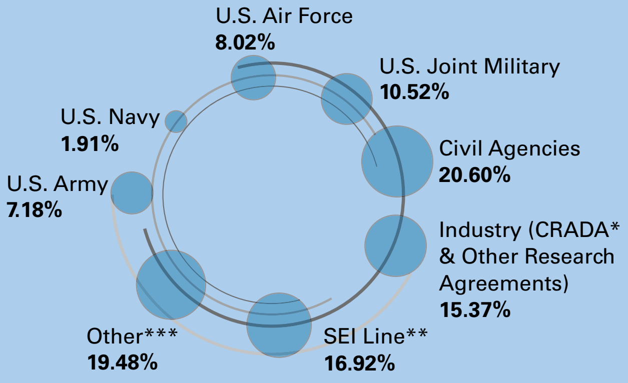
Quality software that is produced on schedule and within budget is a critical component to U.S. defense systems, which is why the U.S. Department of Defense (DoD) established the SEI in 1984. Since then, the SEI has advanced software and systems engineering principles and practices, while serving as a national and international resource for the software and systems engineering communities. As an applied research and development center, the SEI brings immediate benefits to its research partners and long-term benefits to the software industry as a whole.

Operated by Carnegie Mellon University—a global research university recognized worldwide for its world-class arts and technology programs—the SEI operates at the leading edge of technical innovation. The SEI's core purpose is to help organizations improve their capabilities and to develop or acquire the right software, defect free, on time, and on budget, every time.

The SEI offers solutions to customers in the areas of:

- Acquisition
- Process Management
- Risk
- Security
- Software Development
- System Design

The SEI's technical focus areas, together with its outreach activities, are aimed at meeting the defined software engineering needs of the DoD. Within these areas of work, the SEI collaborates with defense, government, industry, and academic institutions to continuously improve software-intensive systems. The SEI's body of work in technical and management practices is focused on developing software right the first time, which results not only in higher quality, but also predictable and improved schedule and cost.



* cooperative research and development agreement—an agreement with an industry or academic collaborator

** funding provided by the Office of the Under Secretary of Defense for Acquisition, Technology, & Logistics—the SEI's primary DoD sponsor—to execute the SEI technical program

*** course fees, conference fees, and other recovered costs

Growing Architecture Competence

While researchers have thoroughly examined the technical aspects of effective software architecture, the qualities necessary to make an effective architect have remained relatively unstudied. Members of the SEI Software Architecture Technology (SAT) team felt that by studying “architecture competence” they could learn how to promote it. Their goals were to identify the measurable factors that contribute to architecture competence in individuals and organizations and to develop an instrument for evaluating these factors. They described their research in the technical report *Models for Evaluating and Improving Architecture Competence*, presenting basic concepts and four models for explaining, measuring, and improving the architecture competence of an individual or a software-producing organization. The authors explained how they could apply the four models to create an evaluation instrument to measure an organization’s architecture competence. Such an evaluation would benefit organizations that acquire, service, or develop software systems.

Also emerging from the SAT team’s work was the Architecture Competence Workshop conducted at the SEI in June 2008, where accomplished practitioners from government, academia, and industry discussed key issues in assessing and improving architectural competence. Through the workshop, the team hoped to understand what leading organizations were doing in the area of architecture competence.

Opening speakers described their organizations’ approaches for promoting architecture competence. Raytheon, for example, has an organization-wide competence improvement project that includes governance by an Architecture Review Board, a formally defined Raytheon Certified Architect Program, and the standards-based Raytheon Enterprise Architecture Process. Boeing is improving its architecture competence by introducing key practices such as architecture evaluation and architect certification. Boeing issues Software Architect Certificates in specific domains and holds an annual conference, where software architects network and share ideas. Raytheon and Boeing both engage SEI technology, such as the Architecture Tradeoff Analysis Method and the Quality Attribute Workshop, to promote best architecture practices.

Through the workshop, the SAT team also hoped to get feedback on their in-progress assessment instrument. This questionnaire is based on the architecture competence framework developed earlier by the team and focuses on what an organization should do if it is serious about incorporating architecture practices. The workshop formed working groups that provided positive input and suggestions for questions and improvement.

The SAT researchers’ work has reinforced the notion that while much remains to be done to define and measure architecture competence, the time for pursuing it has definitely arrived. ■

2008 Independent Research and Development Awards

The SEI annually undertakes several independent research and development (IRAD) projects, which are chosen based on their potential to mature or transition software engineering practices and set new directions for SEI work. The following IRAD projects were completed in FY2008:

- Assurance Cases for Medical Devices
- Mechanism Design
- Understanding the Relationship of Cost, Benefit, and Architecture
- A Software System Engineering Approach for Fault Containment
- Modeling Stakeholder Requirements for Integrated Use in Both Process Improvement and Product Development

To read the report, visit www.sei.cmu.edu/publications/documents/08.reports/08tr025.pdf

Program Merger Enhances Capabilities in System Structure and Behavior

In summer 2008, the SEI Product Line Systems and Dynamic Systems programs merged to create the new Research, Technology, and System Solutions (RTSS) Program. RTSS positions the SEI to provide more complete capabilities for predicting and bounding the structure and behavior of software-reliant systems.

"By combining these two groups, we bring together a strong team of innovative and productive researchers," said Paul Nielsen, SEI Director and CEO. "We will have a stronger concentration of both talent and funding to address the needs we see in architecture, large and ultra-large systems, model-based engineering, software assurance, product lines, and more."

For example, three initiatives came together to form the Architecture-Centric Engineering (ACE) unit. The separate initiatives, Software Architecture Technology (SAT), Predictable Assembly from Certifiable Code (PACC), and Performance-Critical Systems (PCS), shared a common focus on architecture and quality attributes, yet had their own unique emphasis.

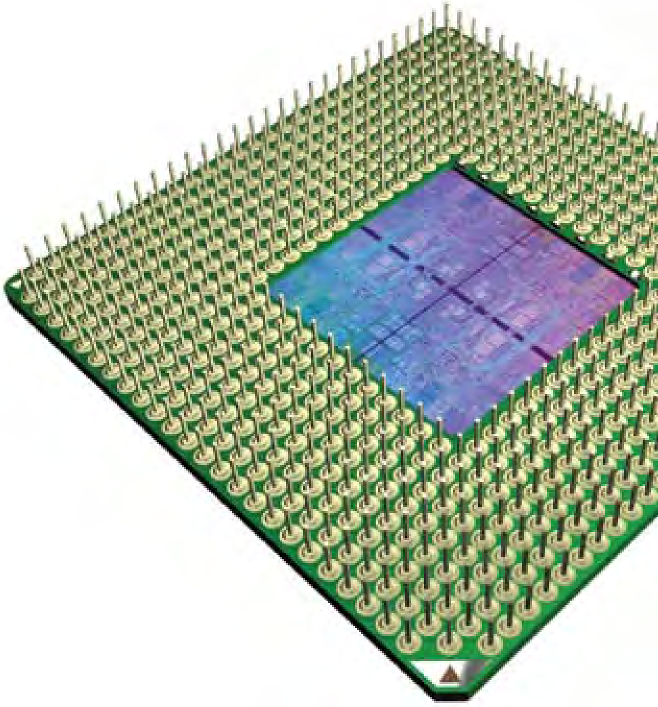
SAT focused on architecture-centric methods, business goals, stakeholder involvement, informal analyses, economics, and widespread transition. PACC used formal architecture and code analyses to understand design space restrictions to allow for predictability. PCS analyzed architecture representations to calculate the dependability and performance of software systems.

By leveraging the commonality and exploiting each group's emphasis, ACE will allow the SEI to focus holistically on using architecture coupled with appropriate analyses and practices to build high-quality, predictable systems. ■

SEI Joins Multicore Association

A multicore processor combines two or more independent cores (normally a CPU) into a single package composed of a single integrated circuit. The increasing availability of processors with many computing cores requires better approaches to developing and deploying concurrent software. As members of the Multicore Association (MCA), members of the technical staff at the SEI are participating in the MCA's Multicore Programming Practices (MPP) working group. This working group is developing a multicore-software programming guide for industry. Participation in the working group will allow the SEI to represent the needs and interests of its stakeholders in the U.S. Department of Defense, government, and industry and communicate the working group's findings to those stakeholders.

SEI researchers are exploring concurrent-programming challenges as they apply to software engineering. They are investigating analytical methods for reasoning about the response time and processor utilization of multicore systems through efficient scheduling, allocation, and synchronization in embedded, real-time, multicore systems. ■



Sharing with Educators

When concepts for effective software engineering are included in college curricula, they are disseminated on a fundamental level with far-reaching ramifications. To promote such inclusion of proven methods and practices, two SEI teams have conducted workshops for instructors in computer science and software engineering.

The first Predictable Assembly from Certifiable Code (PACC) Workshop for Educators was held at the SEI in August. PACC technology promotes accurate predictability. For example, it enables engineers to predict that robots will meet their strict performance deadlines or that medical devices will comply with safety requirements. Predicting the observable executing system behavior of assemblies of software components—from the properties of those components—is achieved through techniques that the PACC team develops. Such prediction requires that the properties of the components are rigorously defined and trusted and can be certified by independent third parties.

The workshop focused on a closely related concept, predictability by construction (PBC), which purports that if a system can be constructed, it will have predictable runtime behavior. The breakthrough of PBC concepts into the classroom is significant. Through the use of available technologies and theories, PBC can be practically achieved for a variety of system-level properties, such as security, safety, and performance. A tutorial on PBC was held on the first day of the workshop, introducing principles that were then demonstrated through concrete working examples. On the second day attendees discussed how to integrate topics covered in the tutorial into computer science and software engineering curricula.

For five years the SEI has also conducted its annual Software Architecture Workshop for Educators. Participants from across the globe have come to discuss architecture concepts crucial to successful software and system development and their delivery into college classrooms. In its early years, the workshop offered introductory coursework and discussion focused on raising awareness regarding good architecture.

In August 2008 the workshop offered the advanced two-day course Software Architecture Design and Analysis, which provides in-depth coverage of the concepts needed to make effective design decisions and to successfully analyze a software architecture relative to desired system qualities. As in previous years, the third day involved sharing ideas on how attendees might incorporate course topics and other architecture-centric design principles into their curricula. Conductors of this year's workshop noted how its influence had deepened and expanded. All participants reported the incorporation of architecture-centric concepts into their curricula; repeat attendees shared thoughts on how previous workshop topics had been applied in their programs; and discussions were much more in depth and sophisticated than when the workshop began. ■

SOA Research

In 2008, the SEI inspired work to further the investigation of several key issues identified in its service oriented architecture (SOA) research agenda. Led by the SEI, a team of internationally known SOA researchers developed a research agenda in 2007. The SEI arranged the agenda in a taxonomy that includes four top-level categories: business, engineering, operations, and cross-cutting concerns. Those categories contain issue areas such as strategy, architecture, monitoring, and governance. In all, more than 50 issues are included.

More than 110 people from government, industry, and academia attended a 2008 workshop on hard problems in SOA hosted by the SEI in association with IBM and Carnegie Mellon University.

SEI researchers began working with Frederic Wenzel from University of Karlsruhe, who is developing a thesis on "Transaction Management in Federated Workflows" at Carnegie Mellon.

The SEI and others organized the Second International Workshop on Systems Development in SOA Environments (SDSOA 2008), which was co-located with the 30th International Conference on Software Engineering (ICSE 2008). This workshop brought together experts to focus on three of the agenda's significant issues: dynamic service composition, design for system qualities, and runtime monitoring and adaptation.

In all, eight workshops have been conducted, and more than 25 papers in conference proceedings have been published on SOA research agenda topics. ■

ULS Systems Research Is Redefining Software Engineering

Two years after publishing the ground-breaking report titled *Ultra-Large-Scale Systems: The Software Challenge of the Future*, the SEI-led research team can see the adoption of its views on the horizon. "A lot of the ideas in the ULS systems report are already here, and people are working on them, but they're not everywhere," Richard P. Gabriel, IBM distinguished engineer and a coauthor of the report, recently told *IEEE Software*. "I think there will be a coalescing of those ideas, and it will be inevitable."

The SEI's work on ULS systems began after the U.S. Army posed the question, "Given the issues with today's software engineering, how can we build the systems of the future that are likely to have billions of lines of code?"

The research team determined that the number of lines of code is only one of several ways in which the scale of systems is growing larger and more complex. The report describes how this increasing scale will force changes to the basic principles and assumptions of software engineering. It recommends research in the areas of human interaction; computational emergence; design; computational engineering; adaptive system infrastructure; adaptable and predictable system quality; and policy, acquisition, and management.

The community response has been positive; the report has motivated research projects around the globe. Linda Northrop, director of the SEI's Research, Technology, and System Solutions Program and lead author of the report, sums up the impact of the ULS systems research this way: "People consistently tell me that the report accurately portrays the challenges that they are seeing. They agree that the inherent characteristics of the ULS systems defy successful use of today's approaches to system development." ■

For more information, visit
www.sei.cmu.edu/uls/

New Webinars Bring SEI to the Desktop

“It’s a convenient way for the SEI to communicate our software engineering best practices directly to practitioners. It’s free, and easy to attend–you don’t even need to leave your office.”

Part of the SEI’s mission is to distribute the knowledge that is created, captured, and applied to the global software and systems engineering community. Technology and the internet allow this information to be presented in more accommodating and interactive ways.

“Between my demanding work schedule and travel and expense cutbacks, it’s challenging to get the training I need to effectively do my job,” said Joanne Mack, statistician and team lead for quality components at the Center for Medicare and Medicaid Services. “Even though the government is reducing spending, they still want a highly trained and competent work staff.”

“That’s precisely why we launched the SEI Webinar Series,” explained Shane McGraw, who coordinates the SEI Software Process Improvement Network (SPIN) groups. “It’s a convenient way for the SEI to communicate our software engineering best practices directly to practitioners. It’s free, and easy to attend—you don’t even need to leave your office.”

Launched in July, the webinar series is proving to be extremely popular. To date, almost 2,000 people have registered to attend a webinar. October’s CMMI for Services presentation attracted nearly 500 participants.

Jeannine Siviy, part of the team that presented the first SEI webinar, Process Improvement in Multi-Model Environments, says that the platform is beneficial to both the community and the SEI’s research staff. “Not only do the webinars allow us to reach people who may not be able to attend the conferences where we are presenting, but the question and answer portion lets us know immediately how our information resonates,” said Siviy. “It’s feedback that we will use to make our materials even stronger and more relevant.”

Mack, who attended the CMMI on the Web webinar, was thrilled with what she learned and the webinar format. “I’m new to the webinar world as well as to the SEI and its coursework,” she said. “But the presentation was easy to use, very informative, and applicable to my job. It helped me look at things I never thought of before.”

The schedule of upcoming webinars—as well as the archive of previous webinars—is posted on the SEI website: www.sei.cmu.edu/collaborating/spins ■

For more information, visit www.sei.cmu.edu/spins?

CERT-DC3 Collaboration Aims for Better DIB Network Defense

The Defense Industrial Base (DIB) comprises 8,700 companies critical to the operations of the U.S. Department of Defense (DoD). Unclassified DIB networks face a range of internet threats capable of evading commercial security tools and defeating security best practices. It is critical for those in charge of these networks to develop and implement a robust and adaptable defense capability.

To meet this challenge, the Office of the Assistant Secretary of Defense for Networks and Information Integration, the Defense Cyber Crime Center (DC3), and the SEI have partnered to better defend this critical national infrastructure. In 2008, the SEI CERT Program began a commitment to research, develop, and implement effective information sharing processes for the DIB community; apply and implement an incident management capability for the DoD and DIB; and, ultimately, transition this capability to the DoD and DIB. ■

New UML Profile Maps to AADL

The Object Management Group (OMG), an international not-for-profit computer industry consortium, in June 2008 released a beta version of a Unified Modeling Language (UML) profile for modeling and analysis of real-time and embedded systems (MARTE). The MARTE extension provides support for specification, design, verification, and validation of real-time and embedded systems. An appendix to MARTE allows mapping to the SAE International Architecture Analysis and Design Language (AADL) and is heavily influenced by the SEI's work on AADL and model-based development.

The OMG MARTE group invited Peter Feiler of the SEI to join in the development of the profile. Feiler is the author of the AADL standard—an industry-established standard for modeling system software architectures that provides a precise, non-ambiguous representation for modeling real-time embedded systems. He says the development of MARTE is an exciting opportunity: "Now there will be a systematic and efficient way to exchange information through the OMG MARTE profile and AADL and vice versa. If you are building an architecture model in AADL, then it can be used in UML MARTE tools. Organizations currently using UML are now offered an additional possibility to use AADL and benefit from the precise modeling and validation of architectural designs that AADL provides." ■

The CERT Podcast Series

Two years ago, Julia Allen started the CERT Podcast Series as a way to provide business leaders with the security information they need. Now, new podcasts are uploaded every two weeks to the CERT website and iTunes. The series has become increasingly popular with more than 80,000 monthly downloads and over 60 titles.

"The podcasts are a very easy transition method," says Allen. "Typically 20 to 30 minutes long, the discussions capture valuable security principles and tactics."

Topics include governing for enterprise security, privacy, insider threat, and risk management and resilience. Podcasts often feature leading industry and government security experts alongside CERT researchers.

"We've also discovered that the podcasts are a great way for us to draw in practitioners," says Allen. "Once they hear the information, they want to read more, take training, and become further engaged with the topics."

VTE Helps DoD Meet Remote Training Requirements and Cut Costs

Since the approval of DoD Directive 8570.01 in December 2005, DoD organizations have had to scramble to identify new and better avenues for training. The directive requires the training and certification of all information assurance technicians and managers to meet DoD baseline requirements related to their jobs. This means roughly 100,000 DoD personnel require training and certification.

Unfortunately, many DoD personnel, particularly members of the armed forces, find themselves in forward-operating bases and other situations where traditional, classroom-based training is difficult if not impossible. In increasing numbers, DoD organizations are turning to CERT's Virtual Training Environment (VTE) to bridge this training gap. VTE provides rich media instruction and hands-on training labs to remote students over the internet. It enables students to access high-quality training on security, computer forensics, and incident response anywhere in the world, with only a web browser and an internet connection.

"The power of the VTE distribution model is that it can reach students in places other training delivery methods can't," notes VTE team lead Jim Wrubel. "Armed forces personnel have accessed VTE from forward-deployed bases in Iraq and Afghanistan, and they've even accessed VTE from ship-side deployments." Wrubel adds that VTE's 15-minute modules have been designed specifically to help students adapt their training to meet unpredictable schedules. What's more, VTE training has no "expiration date"—students can access all training modules as often as they want and for as long as they want after completing training. "Because students can keep coming back to the modules and the test network," notes Wrubel, "VTE helps close the gap between learning a concept and using that concept." The result is more effective information security practice in the field.

VTE's hands-on scenario networks have been a particular hit with DoD students. Accessible directly from the student's computer, the networks enable the student to experiment, learn new skills, and practice network security and management techniques without putting live networks at risk. "Imagine," Wrubel observes, "an Air Force firewall administrator who can't practice his or her skills on the live network. VTE enables the administrator to practice firewall configuration and management on the scenario network, as many times as desired, right from his or her desktop."

VTE has been well received by the DoD, and its use is growing. In the past year, VTE delivered approximately 120,000 hours of training. And not only is VTE filling the training need for DoD personnel in far flung locations, it's doing so at considerable savings to the DoD: VTE-based training saves the DoD 84 percent per student served compared to traditional classroom delivery. Even better for the DoD, this savings comes at no cost to effectiveness. Certification rates for students accessing VTE for training are equal to those of students taking classroom training. ■

For more information, visit
www.cert.org/training/vte_description.html

OKLAHOMA
Amarillo
Albuquerque
NEW MEXICO
ARIZONA
Phoenix
Tucson
Roswell
Las Cruces
El Paso
Lubbock
Fort Worth
Dallas
Abilene
Waco
TEXAS
San Angelo
Austin
San Antonio
Galveston
Laredo
Corpus Christi
Brownsville
Ciudad Juarez
Nogales
Hermosillo
Guaymas
Chihuahua
Rio Grande
Nuevo Laredo
Novojoa
Los Mochis
Monterrey
Culiacan
Torreon
Saltillo
Matamoros
Durango
Ciudad Victoria
Gulf of California
BAJA CALIFORNIA
Paz
Mazatlán
MEXICO
Tampico
San Luis Potosi
León
Guadalajara
Puerto Vallarta
Bay of Campeche
Mexico City
TEOTIHUACAN
Colima
Veracruz
Campeche
Popocatepetl 17,887
Puebla
Ixtapa
Villahermosa
Acapulco
Oaxaca
Tuxtla Gutierrez
Gulf of Tehuantepec
GUATEMALA
Guatemala
CENTRAL
TECNOLÓGICO DE MONTERREY

Mexican TSP Initiative Shows Early Results

Two years after the Mexican government launched its unprecedented program to build a national reputation as a provider of IT products and services using the SEI Team Software Process^{SM} (TSP^{SM}) methodology, early results from pilot projects show an increase in high-quality, low-defect software developed on schedule and with improved team productivity.

These improvements are the result of a strategic alliance forged in 2006 between the SEI and Mexico's leading private university, Instituto Tecnológico de Estudios Superiores de Monterrey (Tec de Monterrey), and enthusiastically supported by the Mexican national government, to advance the state of software engineering practice. The goal of the alliance is to position the Mexican software industry as an international competitor in the global IT outsourcing market by introducing TSP as a component of Mexico's Program for the Development of the Software Industry (PROSOFT).

While industry statistics show that over half of all software projects are more than 100 percent late or are cancelled, in these TSP pilot projects, teams delivered their products on average 2 percent later than they had planned, with some as much as 27 percent earlier. Key to schedule success in the pilot TSP teams was overall high product quality; several TSP projects had no defects in system or acceptance test.

Softtek, a global provider of IT and business process services, participated in the pilot TSP projects and had a defect rate of 0.038 per thousand lines of code.

TSP has also helped to motivate development staff and management. Developers said they prefer the work environment of a TSP team. Management appreciated the depth of the data and the reliability of status reports. Low worker attrition, a relative strength of Mexico, was not only maintained, but enhanced. One company survey of employees found the TSP pilot team to have the highest job satisfaction in the plant.

Initially developed at the SEI by Watts Humphrey, TSP is a process technology that guides teams in reducing time to market, increasing productivity, improving cost, schedule performance, and product quality, accelerating process improvement, and reducing professional staff shortages.

A TSP team has an error rate in deadlines to deliver projects of -10 percent to 5 percent, whereas those without TSP/PSP have an error rate of 140 percent. TSP works in conjunction with the Personal Software Process^{SM} (PSP^{SM}), through which individual engineers can measure and enhance their performance. Both were created as a way to bring CMMI principles to teams and individuals.

"You need to differentiate yourself to compete. Mexico plans to differentiate itself through its largest competitive advantage—the TSP," said Ivette Garcia, the Director of Mexico's Digital Economy. The competitive advantage will come through reduced development time, superior quality, real-time interaction, lower attrition rate, and trust in Mexico's high-performance knowledge workers and teams.

As one of the next steps in the national initiative, Tec de Monterrey is piloting not only an accelerated process improvement method using TSP to implement CMMI called TSP-Based CMMI Accelerated Improvement Method (TC-AIM) but also a TSP organizational evaluation and certification (TSP-OEC). TC-AIM will make CMMI process improvement accessible to small- and medium-size enterprises (SMEs). Organizational certification will provide objective insight into the performance of an organization's products and projects. Taken together, TC-AIM and TSP-OEC will make process improvement and CMMI recognition cost effective for the SMEs. ■

For more information, visit
www.sei.cmu.edu/tsp/

ASSIP

The Army Strategic Software Improvement Program (ASSIP) is a partnership between the U.S. Army and the SEI aimed at promoting an integrated software and systems engineering approach to the Army's acquisition of software. Several Program Executive Office and Program Manager's Office staff members with experience in ASSIP efforts offered their views of the impact of ASSIP.

"The ASSIP effort provided us confidence that we were requesting the right information from our vendors. ASSIP also expanded the value of the vendor information and metrics that we request."

Steve Waldrop
Software Branch Chief
Program Manager's Office
Heavy Brigade Combat Team

"At PEO Aviation we are seeing practical application of the knowledge gained through the ASSIP efforts as our people are continuously seeking ways to improve the cost, schedule and quality of their respective programs."

Terry Carlson, PhD
Chief, Aviation Commonality &
Interoperability Branch
Program Executive Office, Aviation

"The ASSIP is providing timely, relevant, and value-added software engineering expertise to the PEO-GCS community to enhance our software acquisition processes for the warfighter."

Peter Haniak
Chief System Engineer
Program Executive Office
Ground Combat Systems

Army Commitment to Strategic Software Improvement Grows

Just by looking at the 2008 numbers for ASSIP—the SEI's partnership with the U.S. Army aimed at improving Army software—you can tell 2008 was a good year for the five-year-old program.

Indeed, at six Army sites more than 300 Army personnel attended 26 SEI courses related to software architecture, acquisition, and other skills during the year. Also, the SEI hosted three exclusive educational conferences for Army leadership on current software issues and developments; about two dozen Army executives attended each, including general officers and civilian members of the Army's Senior Executive Service.

But the numbers aren't the real story of the Army Strategic Software Improvement Program's successes.

"In 2008 we really began to see awareness [of ASSIP] grow," said Cecilia Albert, who heads up Army programs in the SEI's Acquisition Support Program. "That's what was most impressive." ASSIP, with its mission of ingraining an integrated system and software engineering approach to the Army's acquisition of the software in its systems, is taking root in the Army's acquisition establishment, Albert said.

Robert Schwenk, the Army's senior software acquisition manager, agrees.

"It's not the numbers," Schwenk said. "It's what they signify—ASSIP is succeeding at providing a forum for Army experts to interact with each other, network, and synergize at a leadership level." That is vitally important to the Army's acquisition community, Schwenk noted, because as software grows in complexity—and consistent acquisition processes grow in necessity—it is only through sustained interaction among Army software experts that the force will be able to assure that it obtains high-quality and effective software products.

In short, the Army's software is improving—because ASSIP is helping establish a stronger, more efficient, and more capable software community within the Army itself. That community of professionals is an organic capability that is beginning to deliver on the Army's strategic needs.

2008 saw continued growth in communication, knowledge sharing, and the trading of software engineering and acquisition lessons learned, Albert said, with meetings every other month of the ASSIP Action Group (AAG). AAG, a group that plans and monitors execution for ASSIP, comprises 11 Army program executive offices (PEOs), four Army software engineering centers, the Army's chief information officer, and the Army Test and Evaluation Center. The SEI acts as both subject matter experts and facilitators for the sessions.

"We know [ASSIP] is having a positive effect on the Army's software program," said Schwenk, "because the PEOs are telling us so. They're saying 'this is a worthwhile effort.' For PEOs carrying ever-growing workloads to seek out and attend the regular AAG meetings and other ASSIP activities speaks strongly to the value ASSIP provides."

The year also saw a scaling up of the Army's interest in learning and applying the SEI's software architecture knowledge through ASSIP. A concerted effort conducted through the SEI helped the Army grow its ranks of software experts trained in the SEI Architecture Tradeoff Analysis Method (ATAM). Army personnel have taken part in about a dozen ATAM evaluations to date. The Army has also seen an added, immediate benefit from the architecture training: The PEOs have used them to reveal software risks early in projects' lifetimes.

All of this, Albert notes, is fulfilling the four-fold intent of ASSIP: foster migration to model-based system and software acquisition process improvement; institutionalize broad-based oversight, management, and technical expertise; apply an integrated system- and software-engineering approach to Army acquisition; and systematically incorporate lessons learned, best practices, and new technology into policies, practices and processes.

"It is exciting to see the increasing visibility software is getting across the Army through its strong commitment to ASSIP," Albert said. ■

For more information, visit
www.sei.cmu.edu/programs/acquisition-support/

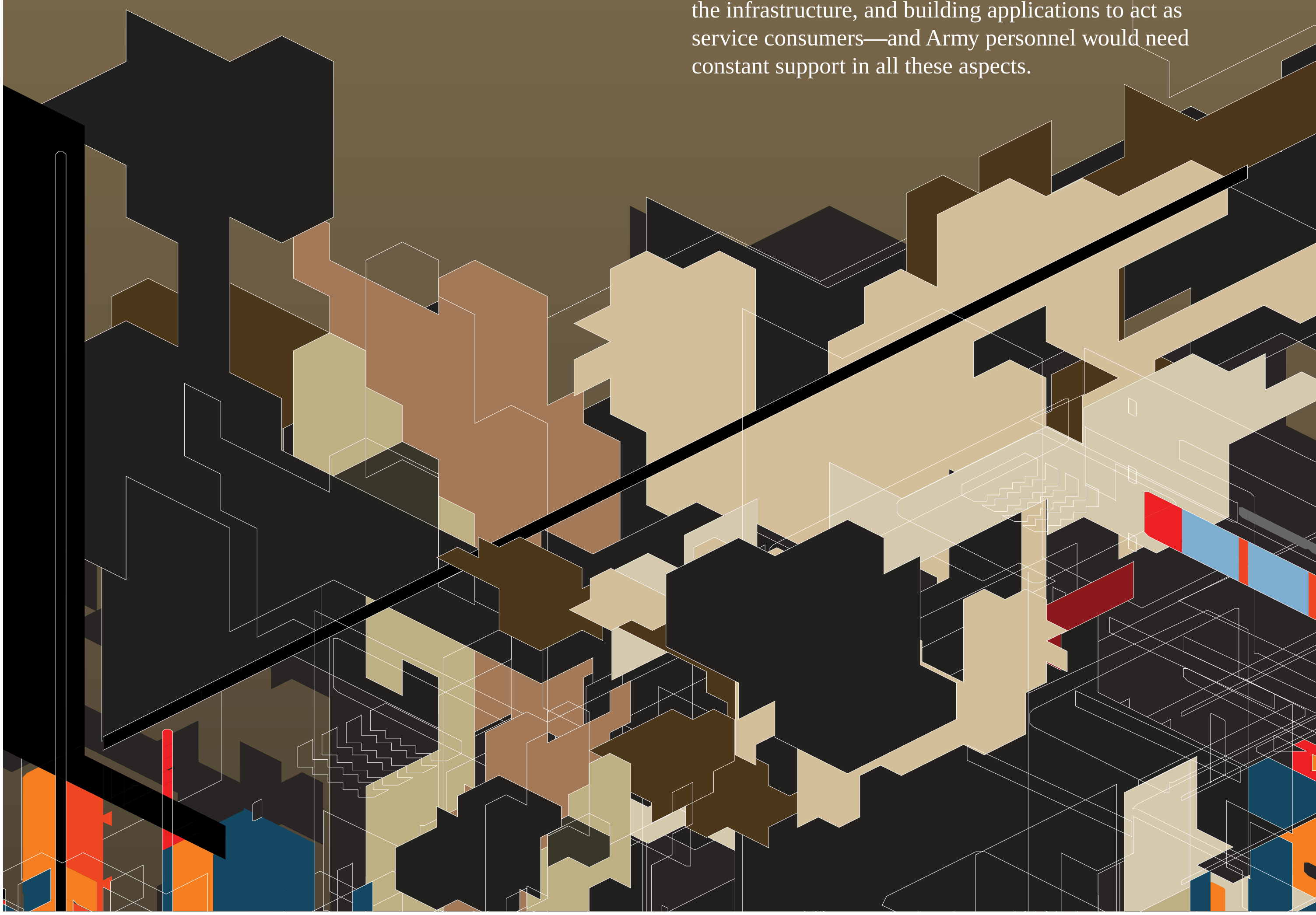
SMART Evolves as Needs Emerge

The story of the Service Migration and Reuse Technique (SMART) and the family of techniques that developed from it is one that illustrates what the SEI does best—engaging with a customer, identifying a need, developing a tailored solution, and subsequently generalizing the solution.

The story begins with the original SMART technique and charts its continuous evolution, all in response to an organizational need to reuse code from legacy systems and transform it into services useful to an organization. Migrated legacy systems have plenty of potential as services that can be reused throughout an organization—customer lookup, account lookup, and credit card validation are some examples.

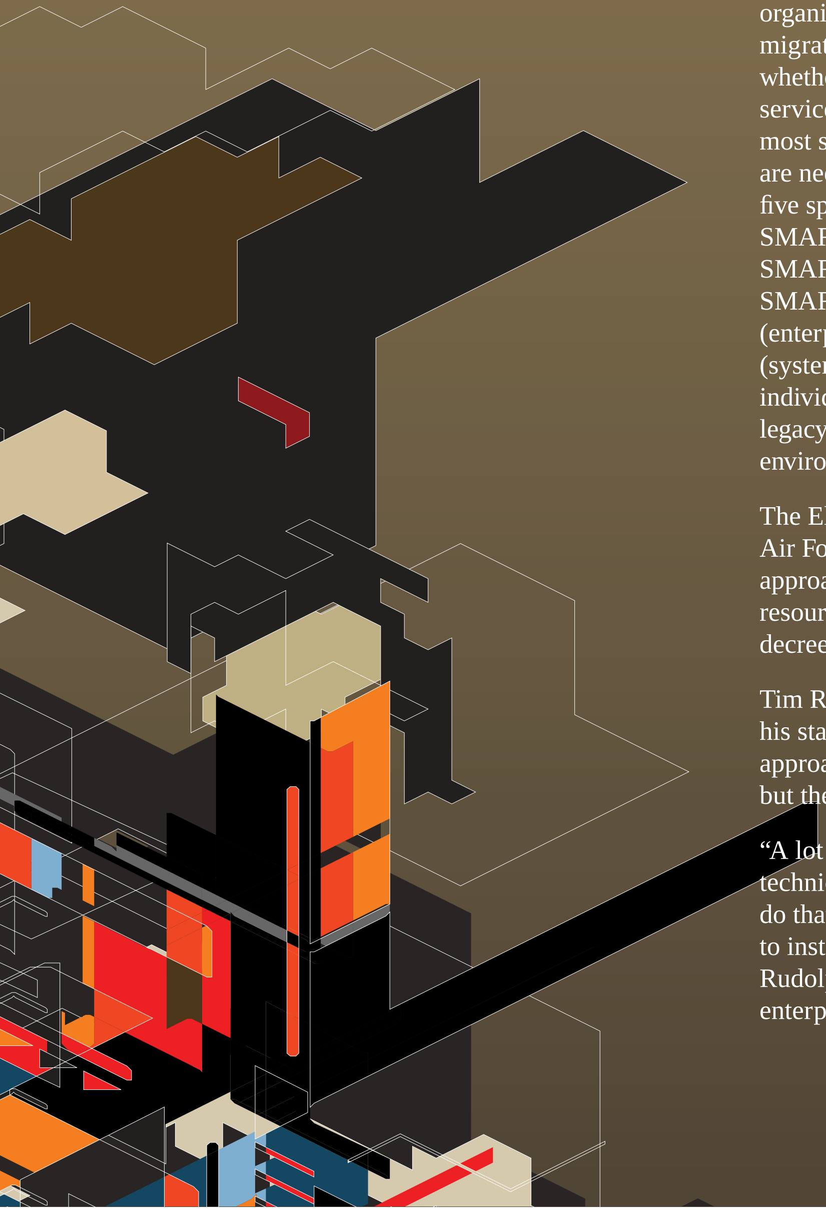
"We don't invent processes that no one uses. We, in fact, look at real needs and respond to those needs," explained Grace Lewis, technical lead for SEI SMART and system-of-systems engineering research. This pragmatic approach is one reason that many organizational leaders—after migrating a single system or implementing a single pilot—then adopt SMART principles across the board.

Earlier this year, a team of engineers from the SEI worked with a division of the U.S. Army to help migrate a legacy command and control system to a service-oriented architecture (SOA) environment. The SEI team soon realized that the system in question had multiple components—they were responsible for implementing services, establishing the infrastructure, and building applications to act as service consumers—and Army personnel would need constant support in all these aspects.



This led the SEI team to revisit its standard approach to service migration that focuses on the service provider—SMART—and refine it to one that would encompass a full service-oriented system. From that need, SMART-SYS was born.

Another member of the SMART family of tools developed this year also saw its impetus in work that the SEI did in helping a government organization migrate a legacy system.



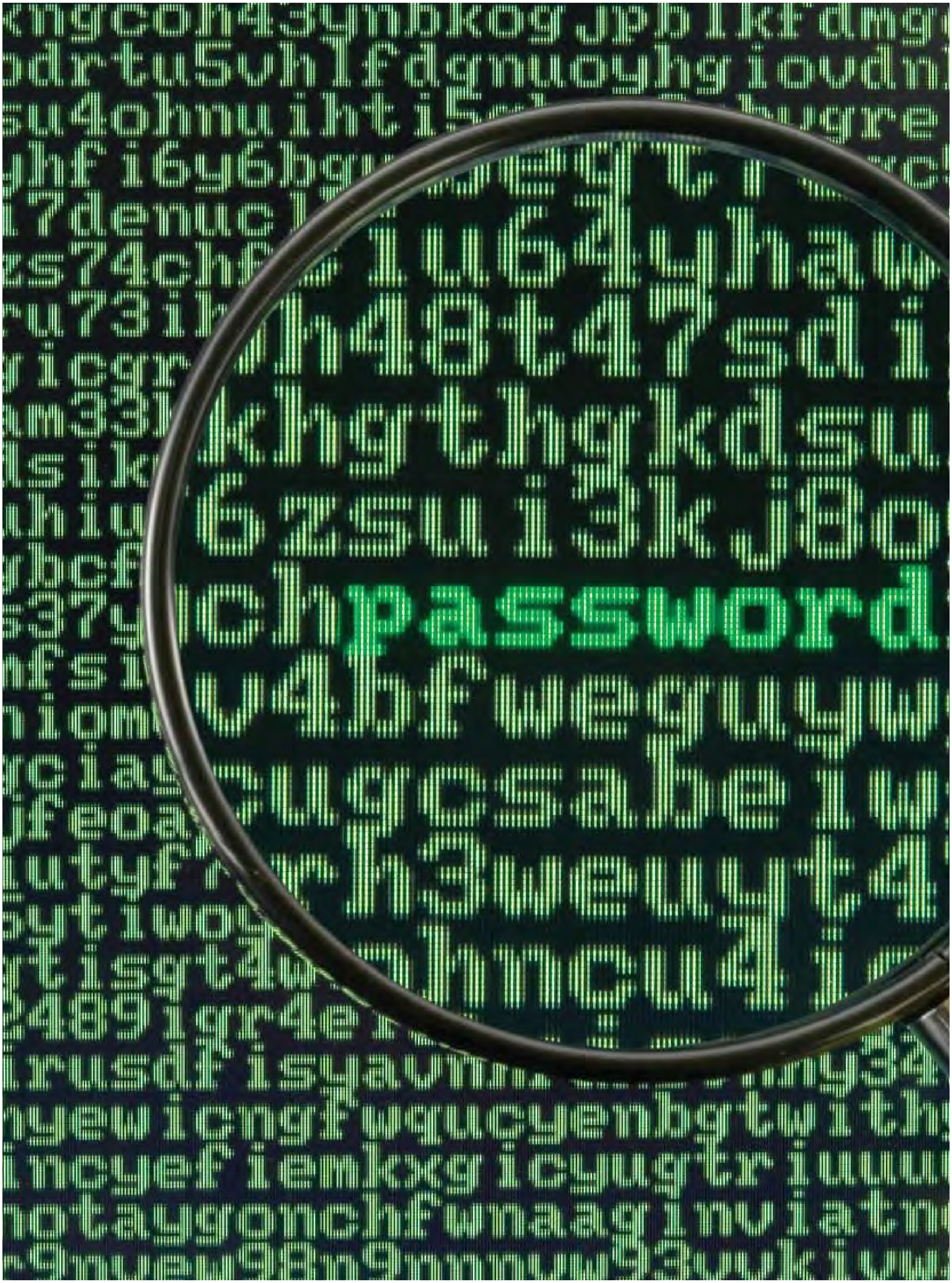
“The system was bureaucratic. It was big. It had rules and regulations and requirements to move through it. The organization had to understand that environment in much greater detail,” explained Patrick Place, a senior researcher at the SEI. To meet those needs, the SEI team again altered its approach and developed SMART-ENV (environment), which focuses on helping an organization understand the target SOA and identify associated costs and risks before migrating.

SMART was developed three years ago to help organizations address important issues before migrating a system to an SOA environment—namely whether it is realistic to migrate these systems to services. And, if so, what services would make the most sense for that organization and what resources are needed. In all this year, the SEI developed five spin-offs or family members from its original SMART tool: SMART-MP (migration pilot), SMART-SMF (service migration feasibility), SMART-ENV (environment), SMART-ESP (enterprise service portfolio) and SMART-SYS (system). All were in response to customers with individualized needs, but a common goal: migrating legacy systems to service-oriented architecture environments.

The Electronic Systems Center (ESC) of the U.S. Air Force is at the forefront of adopting the SMART approach based on experiences migrating a human resources system that managed such tasks as awards, decrees, and temporary duty leave.

Tim Rudolph, ESC chief technology officer, said his staff members have confidence in the SMART approach because not only did they benefit from it, but they continue to help shape it as it matures.

“A lot of these steps [in the SMART process] are less technical and more about behavior and processes. To do that SOA migration properly, it takes some work to institutionalize those competencies,” explained Rudolph. “SMART is an important part of our overall enterprise systems engineering process.” ■



password

Cyber Storm Simulates Network Attack

For a handful of days in March 2008, chaos reigned. Customer support centers at government and commercial organizations were inundated with phone calls reporting problems: a new piece of malicious code that was stealing user names and passwords or a power outage that shut down subway systems.

If left unchecked or mishandled, these incidents could snowball into the types of problems—loss of internet connection, network breaches, transportation system meltdowns—that bring organizations and countries to a standstill. And to almost everyone involved, except for a select group of insiders who monitored every email and phone call, these scenarios were real. The insiders tracked whether, if laws were broken, the company enlisted an outside agency such as the FBI to begin an investigation, and they documented any security measures that were implemented.

This pseudo-cyber attack known as Cyber Storm is conducted every two years and is coordinated by the U.S. Department of Homeland Security's National Cyber Security Division with support from the Software Engineering Institute's CERT® Coordination Center (CERT/CC) and others. It tests government and organizational readiness for real events.

"Cyber Storm is a concerted effort by an adversary to cause harm and measure how government entities and organizations respond to it," explained Marty Lindner of the CERT/CC, who serves as both architect and one of the behind-the-scenes controllers of Cyber Storm during the exercise. This year, the exercise spanned five countries; 18 federal cabinet-level agencies, including the Department of Defense and the Department of Justice; nine states; and 40 private-sector companies. Lindner said that he and others create the scenarios from a compendium of real-life scenarios designed to exploit a gap in policy or a misstep in the chain of response.

These tests are necessary in the current global climate. In 2007, federal agencies reported more than 5,600 cases of computer attacks, intrusions, probes, and plantings of malicious code.

Microsoft helped plan and participated in both Cyber Storm exercises.

"We typically get involved at the very early stages of exercise planning. Our products and technology touch a lot of different sectors and different systems," explained Jerry Cochran, principal security strategist at Microsoft.

The company's involvement was twofold this year. First and foremost, Microsoft's Security Response Center (MSRC) played a key role as an exercise player—responding to security incidents 24/7 as they would in the real world. Cochran also served with Lindner behind the scenes as both an exercise planner and a controller. As a designated controller, he monitored the exercise, fielded rerouted calls—taking any steps to make the exercise appear as real as possible. "A controller fills in the gaps. Sometimes you might be playing the role of a consultant or mimicking representatives from IT sectors that aren't in the game," Cochran explained.

As Cochran sees it, each time that Microsoft participates, lessons are learned and the company is better prepared. And the expansive global involvement this year allowed Microsoft to measure incident response from an international perspective. One lesson Microsoft believes all participants learn by participating in the exercise is that to manage major incidents, it is essential to have established relationships. "In some cases, those partnerships are with competitors in the industry," Cochran said. "From a security-response standpoint, your competitors might be the best partners. In cyber incident response we are all working together for the same cause—our customers and the resiliency of the information infrastructure."

Although similar exercises had been conducted previously, the first Cyber Storm was held in 2006, and it tested government and industry responses to a range of would-be catastrophes. Lindner, who also coordinated that exercise, said that it included hundreds of passengers at airline ticket counters whose names suddenly appeared on no-fly lists, failed railway switches, and a power outage at the Port Authority of New York and New Jersey.

For that exercise, the CERT/CC coordinated efforts with more than 100 public and private organizations in five different countries. The federal agencies investigating the threat traced it back to Lindner, who served as prime perpetrator. "In Cyber Storm I, they arrested me. The Secret Service wanted to handcuff me," Lindner said.

Fortunately, it was just an exercise. ■

For more information, visit www.cert.org

The I in Integration

Beginning in 2008, the Capability Maturity Model® Integration (CMMI) served as a foundation for increased efforts focused on truly integrating software development, software acquisition, and services delivery. "We leveraged the I in integration this year," said Bill Peterson, SEI Software Engineering Process Management program director. "The full CMMI Product Suite weaves together the core principles of CMMI for Development to extend to CMMI for Acquisition and in 2009 to services delivery. With this product suite, we are able to maximize the synergies among the CMMI models."

CMMI for Services—Releasing in 2009

The SEI has seen a growing demand for process improvement in the services sector, which makes up more than 80 percent of the U.S. and global economy. Service organizations—in such areas as healthcare, IT, education, finance, or transportation—have needs and interests that are different from those of development organizations, yet the CMMI model has a track record of effective techniques to improve process capability. CMMI for Services (CMMI-SVC) was designed to provide guidance specifically for organizations providing services. The best practices in CMMI-SVC cover a wide variety of services and are flexible enough to complement models designed for a specific service, such as IT.

CMMI-SVC shares some best practices with CMMI for Development (CMMI-DEV), which provides help to development organizations. Such shared content enables organizations that both develop products and deliver services to use complementary models to improve their capabilities.

Based on pilots with SEI Partners since October 2006, CMMI-SVC is proving valuable for service organizations in improving processes. This in turn can lead to lower costs and better satisfaction for customers and end users. The SEI will release the CMMI-SVC model at SEPG North America 2009 and on the SEI website in March 2009.

CMMI and Six Sigma: Partners in Process

Over the years, the SEI has witnessed organizations struggling with the implementation of process improvement. In some instances, organizations viewed CMMI and Six Sigma as competing approaches rather than a synergistic combination that can yield superior performance. Indeed, some abandoned one approach for another, creating a churn yielding no improvement, delayed production schedules, increased costs, and unhappy employees.

To leverage the best impacts of combining approaches, the SEI began development of a CMMI-Six Sigma Certification. The SEI program will be able to help organizations achieve increased return on investment, better software quality, and development of highly skilled leaders who will be trained to effectively guide their organizations to improved performance using the unique body of knowledge and skills encompassed by the certification program.

During 2009, the community will be asked to take part in the development and review of the CMMI-Six Sigma Body of Knowledge. The focus will be on how to merge the strategic CMMI framework with the Six Sigma tactical toolset (including DMAIC, Lean, and Design for Six Sigma) for performance improvement. The program will be based on leading best practices in measurement and analysis, Six Sigma, and CMMI.

"Significant synergies and energies come from putting CMMI and Six Sigma together," says the SEI's David Zubrow, technical lead for CMMI-Six Sigma initiatives. "Indeed, we have seen substantial beneficial impact on the implementation of high-maturity practices, especially for process performance modeling, through the use of Six Sigma techniques." That's where the SEI comes in. The certification program will provide opportunities for individual instruction, model training, team training, and Six Sigma training to build the workforce.

Jefferson Welch, manager of the certification program at the SEI, emphasizes that the SEI is not trying to replicate Six Sigma certification. "What we have created is a powerful combination of the two. With a certification in place, there are benefits to the organization in terms of transforming, enhancing, and improving the quality of work from the individual perspective." ■

The SEI has seen a growing demand for process improvement in the services sector, which makes up more than 80 percent of the U.S. and global economy.

CERT Forensics Team Helps Law Enforcement Agencies Fight Cyber Crime

It all began with the Iceman case. A former computer security consultant, Max Ray Butler (also known as "Iceman"), was allegedly attacking computers at financial institutions and credit card processing centers, stealing account information, and selling the data to others. The U.S. Secret Service (USSS), which was leading the investigation into Butler's activities, knew of the CERT forensics team's expertise in cracking sophisticated techniques used by cyber criminals, such as encrypting data to hide evidence. The team assisted the USSS in acquiring and decrypting the Iceman's data, thus providing critical evidence for the government's case.

Through word of mouth and presentations the team gives to law enforcement groups, demand for the team's skills and tools spread to state police departments and other law enforcement agencies from coast to coast. "We are providing operational support to the United States Secret Service, to high-profile intrusion and identity theft investigations, and to investigations of other general computer crimes," said team leader Rich Nolan, a former Drug Enforcement Administration agent. This support work enables the team to see problems in the field first hand and then refine their tools or develop new tools and techniques to solve those problems.

One tool that was developed for a specific case is CCFinder. In cases in which investigators were trying to discover compromised credit card and financial account numbers, the existing tools produced many false positives. CCFinder does a better job of finding and validating account numbers and eliminating duplicate numbers. It also maintains a "pedigree" that shows all the locations in which each number was found. The pedigree reveals how stolen numbers were traded (after an initial theft, financial account numbers are often shuffled, split into chunks, and sold) and can aid in tracing the source of the original theft. CCFinder also handles the problem of the sheer size of recent financial crimes, which had overwhelmed existing tools. "CCFinder was a big deal when we were working with 3 million account numbers," said team member Matthew Geiger. "Then we quickly went from there to 45 million in the TJX case."

Cal Waits takes questions from the media on CERT's role in credit card fraud evidence gathering.

The "TJX case" was the investigation of 11 people who were charged in August 2008 with the theft of more than 40 million credit and debit card numbers from T.J. Maxx, Marshall's, Barnes & Noble, OfficeMax, and other major retailers. The forensics team participated in an electronic crimes task force along with USSS agents and state and local law enforcement. "It was an eye-opening experience participating in a law-enforcement action of that scale, with well-organized simultaneous searches," said Geiger.

U.S. Representatives John Murtha, Mike Doyle, and Jason Altmire recognized the team's efforts on TJX during a visit to Carnegie Mellon University in September 2008. "CERT's role in this landmark case underscores its importance in computer security over the past 20 years," said Murtha.

Forensics team members Nolan, Geiger, Cal Waits, Kristopher Rush, and Larry Rogers have multiplied their effectiveness by training the USSS, the FBI, the Department of Defense cyber crime lab, and other law enforcement groups in their tools and techniques. The training is done live on site at the SEI and also via CERT's Virtual Training Environment (VTE), a secured, self-paced, web-based training lab. Authorized members of law enforcement groups can access a number of forensics tools developed by the team on VTE.

"Our primary work is research, but the application of it in real-world cases is what's really gratifying," said Nolan. "A white paper is nice, but locking people up is better." ■

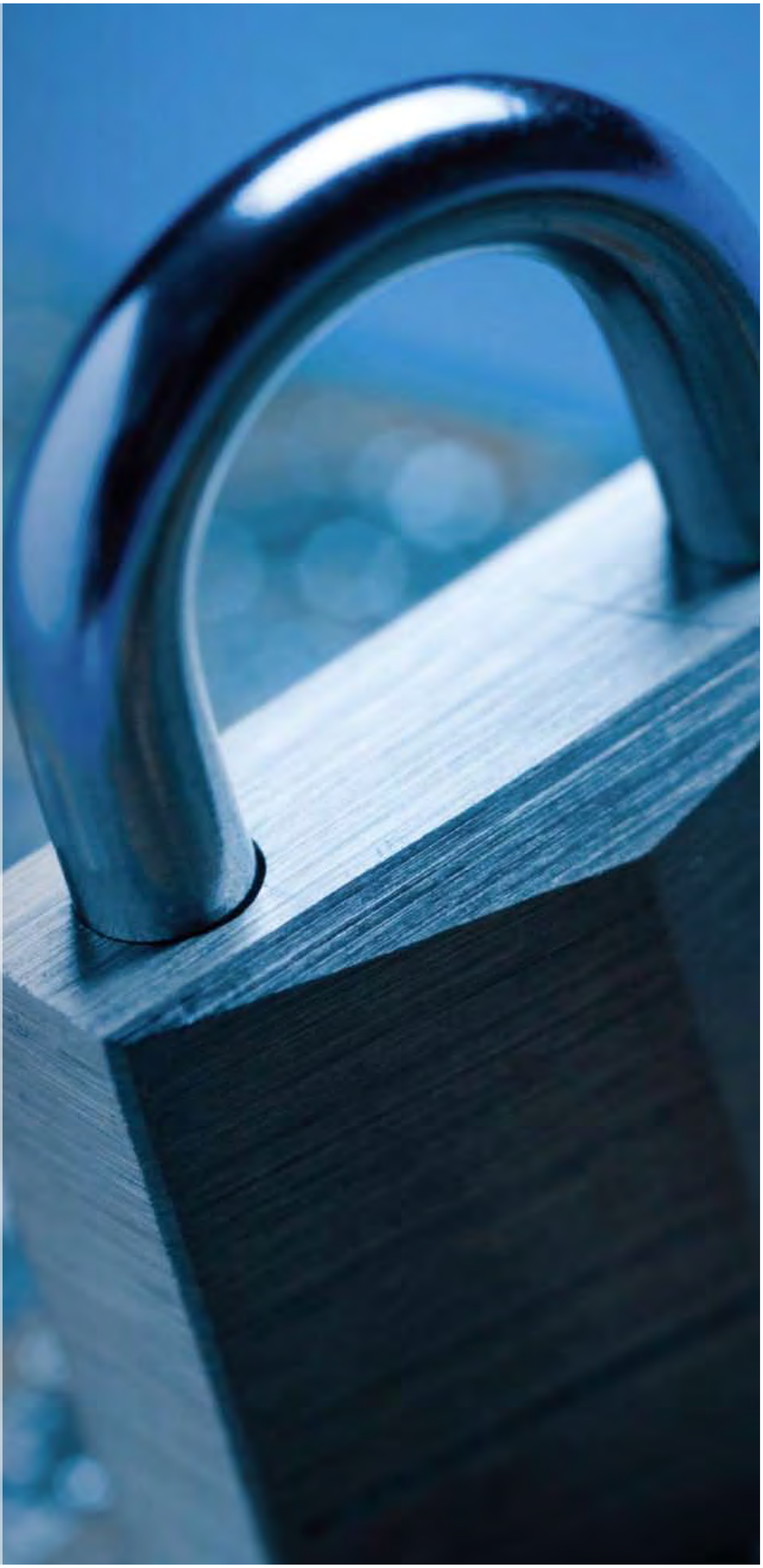
Survey Seeks to Shape the Future of Computer Forensics Education

Proper handling of digital evidence is essential to the successful prosecution of computer-related crimes. The discipline of computer forensics, however, is still in its infancy. A coherent, standardized approach to computer forensics education remains on the horizon.

As a first step toward standardization, CERT forensics team members Cal Waits and Larry Rogers undertook a 2008 survey of the current state of the practice. "The idea grew out of our engagement with members of the federal law enforcement and private sector communities," says Waits. These communities had access to forensics training, but, Waits notes, "they found it to be piecemeal and vocational in nature."

Waits surveyed the federal law enforcement and private sector communities, including the financial sector, to identify needed roles in the forensics field and catalog the skills required to perform these roles. The next step will be to work with the Information Networking Institute at Carnegie Mellon University to plan and develop a model curriculum, based on Waits' findings, suitable for use at degree-granting institutions. Waits' and Rogers' work will be detailed in a forthcoming SEI technical report.

For more information, visit www.cert.org/forensics/



RISK

The CERT Secure Coding Initiative

As software becomes more complex and software security moves closer to the forefront of organizational plans, a means of defining what constitutes a secure system and assuring achievement of this standard is required. Attacks aimed at networked software systems are directed at governments, corporations, educational institutions, and individuals; and they can result in financial loss, the loss and compromise of sensitive data, system damage, and lost productivity—all enabled by simple software vulnerabilities. One way to combat this growing problem is through secure code. But what makes code secure?

The CERT Secure Coding Initiative, spearheaded by Robert Seacord, a senior member of the SEI technical staff, is building a comprehensive approach to secure software development in the C, C++, and Java programming languages. The cornerstone of this approach is the development of secure coding standards for each language. Seacord asserts that "security must be understood for organizations to embrace it—secure coding standards promote adoption by providing a precise and measurable definition." CERT coordinates development of secure coding standards by security researchers, language experts, and software developers using a wiki-based community process. *The CERT C Secure Coding Standard,* for example, was published in October 2008 as an Addison-Wesley book. Once completed, these standards will be submitted to open-standards bodies for consideration and possible publication.

Developers and software designers can apply these coding standards to their code to create secure systems, or analyze existing code against these standards. In September 2005, the team published *Secure Coding in C and C++*, and since then they have created and licensed courses, published books and papers, collaborated with government and private organizations, and presented at conferences to promote standards that will help improve the quality of software released today and in the future.

One example of collaborative work is *The CERT Sun Microsystems Secure Coding Standard for Java.* Currently being developed with Sun Microsystems, this standard provides guidance for secure programming in the Java Platform, Standard Edition 6 environment. Programmers who adopt the Java standard can avoid vulnerabilities in their Java-based applications. This coding standard is applicable to the wide range of products coded in Java such as PCs, game players, mobile phones, home appliances, and automotive electronics.

However, secure coding standards alone are inadequate to ensure secure software development because they may not be consistently and correctly applied. To solve this problem, CERT is developing an application certification process that can be used to verify the conformance of a software product with secure coding standards. Because this process depends on the application of source code analysis tools, CERT is working with industry partners such as LDRA and Fortify Software, and research partners such as JPCERT and Lawrence Livermore National Laboratory to enhance existing source code analysis tools to verify compliance with CERT guidelines. ■

For more information, visit www.cert.org/forensics/

CMD Aids in Bandwidth Allocation

Today on the battlefield, many types of military personnel—such as operators of unmanned-air and all-terrain vehicles, intelligence operators, and commanders—must communicate on a moment-to-moment basis as conditions on the field change. This critical communication occurs over tactical data networks (TDNs)—series of gateways, servers, unmanned vehicles, and operation centers, connected via mobile, wireless, and ad-hoc mesh networks.

TDNs have finite resources such as limited network bandwidth that all network users and components compete for when exchanging information. Allocating bandwidth effectively has always been a challenging problem, but as TDNs become increasingly complex and more closely coupled with moment-to-moment, rational (or self-interested) human decision making, these challenges become daunting. Researchers around the world are investigating the use of market mechanisms to allocate scarce computational resources: Could these ideas be useful in TDNs?

To find out, researchers at the SEI have been developing auction mechanisms for bandwidth allocation in TDNs. In 2006, the SEI showed how auctions can be used to improve the common operating picture in a prototype TDN based on the Navy's LINK-11. In 2007, the SEI joined with Harvard University and the Naval Post-Graduate School (NPS) to demonstrate auction mechanisms for bandwidth allocation in a more complex and demanding TDN testbed developed by the NPS, called the Tactical Network Topology (TNT). TNT links equipment in three locations across the United States and manages all communications among them. The NPS is using TNT to pioneer adaptive tactical networks based on the concepts of 8th Layer, which enables adaptive networking by giving every critical node bandwidth adaptation and small-scale network operation capability. The 8th Layer-enabled hyper-nodes adapt their behavior by exchanging services in accordance with the Valued Information at the Right Time (VIRT) concept.

Alex Bordetsky, the principal investigator and founder of the NPS's TNT testbed, says, "The SEI's work in mechanism design is helping our forces to cross what we call the 'last tactical mile.' It runs from command headquarters to tactical units in remote locations and has information gaps along the way—that's where 8th Layer adaptation comes in. It helps us bridge those gaps—something that becomes more and more important as systems grow more dynamic, performance becomes more critical, and resources dwindle."

Applying auction mechanisms this way is cutting edge, says Kurt Wallnau, one of the SEI researchers investigating computational mechanism design (CMD). According to Wallnau, the TNT arena gave

SEI researchers a chance to demonstrate CMD as a way to develop self-regulating systems where different actors get different allocations based on economic principles. “CMD is all about designing the right incentive structure just like the economics involved in an auction, a voting protocol, or a market. Economics is tailor-made for the kinds of decentralized decision making required by network-centric systems—systems that are not just being used in the military. This problem affects diverse areas from emergency response systems to large city infrastructures,” said Wallnau.

This successful application of CMD research is part of a larger research effort the SEI is leading in ultra-large-scale (ULS) systems—an effort that began in 2006 with the publication of the report titled *Ultra-Large-Scale Systems: The Software Challenge of the Future*. Next, Wallnau’s team of researchers plans to continue working with the NPS and Harvard to develop mechanisms for wireless mesh networks that allow nodes across broken or blocked paths to communicate through “hops”—similar to the moves of tokens in a game of Chinese checkers. Wallnau is confident that the SEI’s research will help there too: “Although CMD is leading-edge research, we believe it’s an engineering discipline waiting to emerge and will soon be on par with performance engineering and safety engineering.” ■

For more information, visit
www.sei.cmu.edu/uls/

Gabriel Moreno, part of the SEI team that worked with the Naval Post-Graduate School, monitors activity on a tactical data network that links equipment spread around the world.

AVSI Chooses AADL for Next Gen Design

Researchers at the Aerospace Vehicle Systems Institute (AVSI) foresaw a problem with building the next generation of complex, software-intensive, safety-critical aircraft systems; as the complexity of the avionics systems continues to increase, they have identified a need for a fundamental change in developing the software and systems for the next generation system aircraft. Through Georgia Tech, AVSI conducted a pre-study of existing technologies that could help with software-intensive systems construction, and the Georgia Tech study recommended adoption of the Architecture Analysis and Design Language (AADL), which was developed at the SEI as a means to conduct model-based development.

“The AVSI project Systems Architecture Virtual Integration (SAVI) focuses on establishing a new way of specifying and integrating increasingly complex aerospace systems. This would reduce the cost and schedule of new airplane development while improving quality, safety, and performance,” says Jörgen Hansson of the SEI. Traditionally, subcontractors responsible for a part of the system would independently develop code or pieces of the system. When the pieces are brought together, the system has already gone far into development, but when you try to integrate all the pieces from the different subcontractors, the integration problems appear.

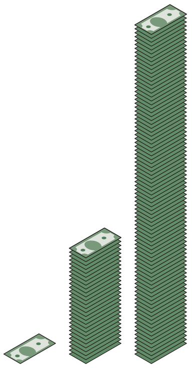
“So the question they are asking,” says Hansson, “is whether there is a way to conduct integration earlier using a model-based approach before the system is being built.” This is where AADL comes in. Using AADL, individual subcontractors can model their pieces of the system with large amounts of implementation detail. “Now I can take that model together with everyone else’s models and integrate them and make sure I get the system behavior I want for areas I determine to be critical,” says Hansson.

This process will allow AVSI to capture many integration faults as early in the development process as possible. The cost of fixing a fault escalates dramatically the later it is uncovered in the development process.

Studies have shown that 60 percent to 75 percent of all system defects are introduced in the system-lifecycle development phases preceding the code development—requirements engineering, system architecture design, and component designs. Yet only a small fraction of these defects, about 3 percent to 8 percent, are detected before code development and system realization; the majority of defects are detected at the time of system integration or later phases.

Correcting late-detected defects incurs significant costs. For example, the costs of correcting defects in the system-integration phase or after the system has been deployed into operation, are 15 to 30 times, and 30 to 110 times higher respectively compared to the cost of the removing the defects early—in the phase in which they were introduced.

“The goal,” says Hansson, “is to do more up-front modeling of the system to mitigate risks and integration problems, save money and time, and possibly allow construction of even larger, more complex systems with this technique.” ■



Costs of correcting defects in the system-integration phase or after the system has been deployed into operation are 15 to 30 times, and 30 to 110 times higher, respectively, compared to the cost of removing the defects early.

AVSI
The Aerospace Vehicle Systems Institute (AVSI) is a consortium comprising aerospace companies—including Boeing, Lockheed Martin, Rockwell Collins, and others—the Department of Defense, and the Federal Aviation Administration. AVSI works to improve the integration of complex subsystems in aircraft.

Securing Web Services in an SOA Environment for the Army SOA Initiative

In 2008, the SEI created a web service certification process for the U.S. Army's Chief Information Office/G-6 (CIO/G-6) organization to address security and provisioning concerns the Army foresees in its development of service-oriented architecture (SOA) environments. The CIO/G-6 organization is responsible for the information management function of the Army.

SOA, according to a definition by IBM, is "the architectural style that supports loosely coupled services to enable business flexibility in an interoperable, technology-agnostic manner." For the Army, and other Service branches in the U.S. Department of Defense, SOA promises a means to realize a vision in which warfighters have a Defense-enterprise-wide capability through which they can choose and assemble services quickly in order to adapt and change to conditions on the battlefield.

Key concerns for the Army in moving toward SOA are information assurance, interoperability, and networthiness, according to Sriram Bala, a member of the SEI team working with the Army CIO/G-6. "The central question is this: If we are to field SOA on DoD networks, how do we assure that it is safe to use," Bala says.

The need for information assurance poses the question of how to protect information and services by ensuring confidentiality, integrity, authentication, availability, and non-repudiation, according to Bala. This level of protection is needed while the information is in storage, processing, or transit and whether it is threatened by malice or accident.

Web service interoperability aims to provide seamless and automatic connections from one software application to another. The networthiness of a web service in an SOA context depends on determining network impact of the web service, developing port and protocol *white list* policies for web service use, conducting network security scans to ensure that web services are not compromising networks, and other factors. White list policies define what a service is allowed to do, according to Ed Morris, another SEI team member.

In 2008, the SEI team created a certification and accreditation process for the Army CIO/G-6 that homes in on these concerns. "The intent of our process is to certify services in order to assure that they are not malicious to the SOA infrastructure that they are deployed on or interacting with," Bala explains.

"We have devised a process that can be executed rapidly to certify and accredit web services—to accomplish these steps in days rather than months," Morris explains. "An Army SOA is expected to be dynamic, and it does no good to be able to assemble services rapidly if those services cannot be certified in a timely way."

This process is robust so that it can "deal with services for which source code is not available," Bala says. "And it is flexible so that it can be modified and institutionalized by other service branches and commercial organizations eventually," he notes.

In addition, the SEI process is "heavily tool-centric," Morris says. It draws on applicable commercial and open-source technologies. Even so, the SEI has found that existing testing tools are inadequate for the job; as a result, the SEI process "includes manual review by sophisticated users to interpret what the tools are telling them," Morris adds.

Now that the process has been created, the SEI team is working with the Army CIO/G-6 to make it operational.

"Our next steps include developing a strategy for testing end-to-end mission threads to integrate certified services to perform the tasks in a mission," Morris says.

SEI Affiliate Program

Through the SEI Affiliate Program, sponsoring organizations contribute technical staff members to the SEI's ongoing effort to define superior software and systems engineering best practices. Affiliates lend their technical knowledge and experience to SEI teams investigating specific technology domains.

Affiliates are immersed in the inquiry and exploration of new tools and methods that promise to increase productivity, make schedules predictable, reduce defects, and decrease costs.

For more information about the SEI Affiliate Program, visit www.sei.cmu.edu/collaborating/affiliates

SEI Partner Network

The SEI Partner Network is an elite group of SEI-trained organizations on the leading edge of software engineering processes and technologies. SEI Partners are licensed to deliver SEI services. SEI Partners provide the following:

- CMMI v1.2 Product Suite Services
- People CMM Product Suite Services
- SCAMPI Appraisal Services
- CERT Information Security Courses
- Implementing Goal-Driven Measurement Course
- Improving Process Performance Using Six Sigma Course
- Designing Products and Processes Using Six Sigma Course
- Software Architecture: Principles and Practices Course
- Team Software Process Services

By delivering services worldwide, the SEI partners provide a critical distribution channel for accomplishing the SEI mission.

In FY 2008, the SEI Partner Network consisted of 387 partner organizations.

For more information about the SEI Partner Network, visit www.sei.cmu.edu/partners/

SEI Conferences & Events

As part of its strategy to apply the latest research, the SEI offers conferences, workshops, and user-group meetings. These events represent technical work and research performed by the SEI and its collaborators in the areas of process improvement, software architecture and product lines, security, acquisition, and interoperability.

Individuals from around the world attend SEI conferences and events to

- connect with industry leaders
- share best practices
- network with peers
- find potential solutions
- gather the latest research and trends in software and systems engineering

Some of the events that the SEI sponsored and co-sponsored are

- Army Senior Leadership Education Program
- FloCON
- SATURN 2008
- SEPG Conference Series
- SMART ULS Workshop
- TSP Symposium

For more information about SEI conferences and events, visit www.sei.cmu.edu/events/

SEI Professional Development Center

The SEI has formed a new Professional Development Center incorporating education, training, and credentialing, all of which enable individuals to benefit from the SEI's research in multiple disciplines.

The center provides continuing education for engineering and software professionals in government, industry, and academia. The SEI addresses professional development needs by:

- designing and developing training that is accessible and effective with classroom, blended, and distance learning
- encouraging and recognizing individual accomplishments in various disciplines through certificate programs
- enhancing individual career opportunities through SEI Certification

In FY2008, the SEI delivered 352 courses, trained 5,990 individuals, and awarded 515 certifications.

For more information about SEI training, visit www.sei.cmu.edu/products/courses/

For more information about SEI Certification, visit www.sei.cmu.edu/certification/

SEI Membership

SEI Membership is a business and knowledge network that connects the SEI with software and systems engineering leaders in government, industry, and academia throughout the world. SEI Membership is designed for software and systems engineering professionals who are interested in priority access to SEI technologies and events. Individuals use the SEI Membership program as a means of networking with other professionals to discuss adoption and implementation of software-engineering best practices and challenges of software and systems engineering.

SEI Members include small-business owners, software and systems developers, CEOs, directors, and managers from business, industry, and prominent government organizations in 36 countries around the globe.

The SEI is the only one of 37 federally funded research and development centers that offers membership to the public.

For more information about SEI Membership, visit www.sei.cmu.edu/membership/

Did you know....

100
Projects on which the SEI collaborated with Carnegie Mellon University

27
Academic customers and collaborators

76
Government customers and collaborators

60
Government acquisition programs receiving on-site support from the SEI

31
Industry customers and collaborators

88
Army leaders attending the Senior Leadership Education Program at the SEI

15,000
Registered attendance at CMMI courses this year

120,000
Hours of training delivered by the CERT Virtual Training Environment

859
Publications & books (respectively) published by the SEI to date.

Paul D. Nielsen
Director
Chief Executive Officer

Clyde G. Chittister
Chief Operating Officer

Leadership, Management, & Staff

SEI Director's Office

The SEI Director's Office ensures the smooth, efficient operation of the SEI. Director and Chief Executive Officer Paul Nielsen and Chief Operating Officer Clyde Chittister build strong, collaborative relationships with leaders in government, industry, and academia, communicating the SEI's vision for software engineering.

SEI Board of Visitors

The SEI's Board of Visitors advises the Carnegie Mellon University president and provost and the SEI director on the SEI's plans and operations. The board monitors SEI activities, provides reports to the president and provost, and makes recommendations for improvement.

Christine Davis-Dittrich
Chair, Board of Visitors; Consultant; Former Executive Vice President, Raytheon Systems Company

Barry W. Boehm
TRW Professor of Software Engineering, University of Southern California; Director, University of Southern California Center for Software Engineering

Claude M. Bolton
Executive-In-Residence, Defense Acquisition University; Former Assistant Secretary of the Army for Acquisition, Logistics, and Technology

William Bowes
Aerospace Consultant: Vice Admiral, USN (Ret.); Former Commander, Naval Air Systems Command, and Principal Deputy Assistant Secretary of the Navy for Research, Development, and Acquisition

Gilbert F. Decker
Consultant; Former President and CEO, Penn Central Federal Systems Company; Former President and CEO of Acurex Corporation; Former Assistant Secretary of the Army/Research, Development, and Acquisition

Philip Dowd
Private Investor; Former Senior Vice President, SunGard Data Systems; Trustee, Carnegie Mellon University

Delores M. Etter
Texas Instruments Distinguished Chair in Engineering Education and director, Caruth Institute for Engineering Education, Southern Methodist University; Former Deputy Under Secretary of Defense for Science and Technology

John M. Gilligan
President, Gilligan Group; Former Senior Vice President & Director, Defense Sector of SRA International; Former CIO for the Department of Energy

Tom Love
Chief Executive Officer, ShouldersCorp; Founder of Object Technology Group within IBM Consulting

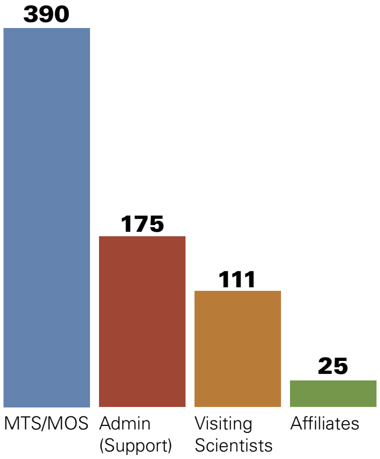
Alan J. McLaughlin
Consultant; Former Assistant Director, MIT Lincoln Laboratory

Michael Reiter
Lawrence M. Slifkin Distinguished Professor, Department of Computer Science, University of North Carolina at Chapel Hill; Former Professor of Electrical & Computer Engineering and Computer Science, Carnegie Mellon University

Donald Stitzenberg
President, CBA Associates; Trustee, Carnegie Mellon University; Former Executive Director of Clinical Biostatistics at Merck; Member, New Jersey Bar Association

SEI Staff

The SEI attracts top talent to implement its expanding objectives, increasing its staff by a third over the past four years. Staff members are permanent, full-time employees; visiting scientists are temporary SEI employees from government, industry, and academia; affiliates are professionals sponsored by their home organizations to work on SEI technical projects.



*Members of the technical staff and members of the operational staff.

John Bramer
Director, Program Development and Transition

Peter Menniti
Director, Financial and Business Services

William Peterson
Director, Software Engineering Process Management

Linda Northrop
Director, Research, Technology, and System Solutions

Richard Pethia
Director, Networked
Systems Survivability

Joe Elm
Acting Director, Acquisition
Support

David Thompson
Director, Information Technology

Key Publications

Young Researchers' Work to Appear in FMCAD Proceedings

Two principal techniques for static analysis of programs—to predict with confidence the programs' runtime behavior—occupy opposite ends of a spectrum. Predicate abstraction (PA) permits construction of detailed models of programs to predict deep semantic properties. Numeric abstraction (NA) permits construction of less precise models but allows reasoning about especially large programs. The challenge is to come up with a technique that allows a smooth combination of the two.

That challenge motivated two young SEI researchers to harness the capabilities of these two techniques. Their research, which has been presented at several workshops and invited talks, was accepted for publication in the *Proceedings of the Eighth International Conference on Formal Methods in Computer-Aided Design (FMCAD).*

"PA is suited for control-driven properties—that doors open and close exactly when they're supposed to, for instance," says Arie Gurfinkel. "NA is suited for data-driven properties—that the temperature sensor never overflows. In reality you don't have programs that just control temperature or doors; you typically have a combination of properties."

"While it is common now for organizations to use one or the other or possibly both processes in sequence, we tried to couple them tightly so that they can run in parallel and work together—one process helping the other," says Sagar Chaki.

Gurfinkel and Chaki performed experiments on open source C programs to determine how to combine PA and NA tightly but in four different combinations in which there are tradeoffs between the scalability of the analysis versus the precision. The paper presents a framework for the four different instances of coupling PA and NA, and each instance is different in terms of how precise and scalable it is.

Chaki presented the paper at FMCAD in November 2008 in Portland, Ore. Preliminary presentations were made at the IFIP Working Conference on Verified Software: Theories, Tools, and Experiments in Toronto, Ontario, Canada; and at the Sixth NASA Langley Formal Methods Workshop, Newport News, Va.

SEI Reports

Christopher Alberts, Audrey Dorofee, & Lisa Marino. *Mission Diagnostic Protocol, Version 1.0: A Risk-Based Approach for Assessing the Potential for Success Parent SEI Program.* www.sei.cmu.edu/pub/documents /08.reports/08tr005.pdf

Christopher Alberts, Audrey Dorofee, & Lisa Marino. *Preview of the Mission Assurance Analysis Protocol (MAAP): Assessing Risk and Opportunity in Complex Environments.* www.sei.cmu.edu/pub/documents /08.reports/08tn011.pdf

William Anderson, Ed Morris, Dennis Smith, & Mary Catherine Ward. *COTS and Reusable Software Management Planning: A Template for Life-Cycle Management.* www.sei.cmu.edu /pub/documents/07.reports/07tr011.pdf

Emanuel R. Baker, Matthew J. Fisher, & Wolfhart Goethert. *Basic Principles and Concepts for Achieving Quality.* www.sei.cmu.edu/pub/documents /07.reports/07tn002.pdf

Len Bass, Paul Clements, Rick Kazman, & Mark Klein. *Models for Evaluating and Improving Architecture Competence.* www.sei.cmu.edu/pub/documents /08.reports/08tr006.pdf

Len Bass, Dionisio de Niz, Jörgen Hansson, John Hudak, Peter H. Feiler, Don Firesmith, Mark Klein, Kostas Kontogiannis, Grace A. Lewis, Marin Litoiu, Daniel Plakosh, Stefan Schuster, Lui Sha, Dennis B. Smith, & Kurt Wallnau. *Results of SEI Independent Research and Development Projects.* www.sei.cmu.edu/pub/documents /08.reports/08tr017.pdf

Philip Boxer, David Carney, Suzanne Garcia, Lisa Brownsword, William Anderson, Patrick Kirwan, Dennis Smith, & John Morley. *SoS Navigator 2.0: A Context-Based Approach to System-of-Systems Challenges.* www.sei.cmu.edu/pub/documents /08.reports/08tn001.pdf

Grady Campbell. *Software-Intensive Systems Producibility: A Vision and Roadmap (v 0.1).* www.sei.cmu.edu/pub/documents /07.reports/07tn017.pdf

CMMI Product Team. *CMMI for Acquisition, Version 1.2.* www.sei.cmu.edu/pub /documents/07.reports/07tr017.pdf

Sholom Cohen & Robert W. Krut. *Proceedings of the First Workshop on Service-Oriented Architectures and Product Lines.* www.sei.cmu.edu/pub/documents /08.reports/08sr006.pdf

Stephen Dewhurst, Chad Dougherty, Yurie Ito, David Keaton, Dan Saks, Robert C. Seacord, David Svoboda, Chris Taschner, & Kazuya Togashi. *Evaluation of CERT Secure Coding Rules through Integration with Source Code Analysis Tools.* www.sei.cmu.edu /pub/documents/08.reports/08tr014.pdf

Audrey Dorofee, Georgia Killcrece, Robin Ruefle, & Mark Zajicek. *Incident Management Mission Diagnostic Method, Version 1.0.* www.sei.cmu.edu/pub /documents/08.reports/08tr007.pdf

Audrey Dorofee, Lisa Marino, & Christopher Alberts. *Lessons Learned Applying the Mission Diagnostic.* www.sei.cmu.edu /pub/documents/08.reports/08tn004.pdf

Robert J. Ellison, John Goodenough, Charles Weinstock, & Carol Woody. *Survivability Assurance for System of Systems.* www.sei.cmu.edu/pub documents/08.reports/08tr008.pdf

Joseph P. Elm, Dennis R. Goldenson, Khaled El Emam, Nicole Donatelli, & Angelica Neisa. *A Survey of Systems Engineering Effectiveness—Initial Results.* www.sei.cmu. edu/pub/documents/07.reports/07sr014.pdf

Peter Feiler & Jörgen Hansson. *Flow Latency Analysis with the Architecture Analysis and Design Language (AADL).* www.sei.cmu.edu /pub/documents/07.reports/07tn010.pdf

Peter H. Feiler & Dionisio de Niz. *ASSIP Study of Real-Time Safety-Critical Embedded Software-Intensive System Engineering Practices.* www.sei.cmu.edu/pub /documents/08.reports/08sr001.pdf

Ashwin Gayash, Venkatesh Viswanathan, Deepa Padmanabhan, & Nancy R. Mead. *SQUARE-Lite: Case Study on VADSoft Project.* www.sei.cmu.edu/pub /documents/08.reports/08sr017.pdf

Fabian Hueppi, Lutz Wrage, & Grace A. Lewis. *T-Check in Technologies for Interoperability: Business Process Management in a Web Services Context.* www.sei.cmu.edu/pub /documents/08.reports/08tn005.pdf

Mark Kasunic. *A Data Specification for Software Project Performance Measures: Results of a Collaboration on Performance Measurement.* www.sei.cmu.edu/pub /documents/08.reports/08tr012.pdf

Mark Klein, Daniel Plakosh, & Kurt Wallnau. *Using the Vickrey-Clarke-Groves Auction Mechanism for Enhanced Bandwidth Allocation in Tactical Data Networks.* www.sei.cmu.edu/pub/documents /08.reports/08tr004.pdf

Grace A. Lewis, Edwin J. Morris, Dennis B. Smith, & Soumya Simanta. *SMART: Analyzing the Reuse Potential of Legacy Components in a Service-Oriented Architecture Environment.* www.sei.cmu.edu/pub/documents /08.reports/08tn008.pdf

Grace A. Lewis & Dennis B. Smith. *Proceedings of the International Workshop on the Foundations of Service-Oriented Architecture (FSOA 2007).* www.sei.cmu.edu /pub/documents/08.reports/08sr011.pdf

Steve Masters, Sandi Behrens, Judah Mogilensky, & Charlie Ryan. *SCAMPI Lead Appraiser Body of Knowledge (SLA BOK).* www.sei.cmu.edu/pub/documents /07.reports/07tr019.pdf

Nancy R. Mead, Venkatesh Viswanathan, Deepa Padmanabhan, & Anusha Raveendran. *Incorporating Security Quality Requirements Engineering (SQUARE) into Standard Life-Cycle Models.* www.sei.cmu.edu/pub /documents/08.reports/08tn006.pdf

Craig Meyers & James D. Smith. *Programmatic Interoperability.* www.sei.cmu.edu/pub/documents /08.reports/08tn012.pdf

Ira A. Monarch, Dennis R. Goldenson, & Lawrence T. Osiecki. *Requirements and Their Impact Downstream: Improving Causal Analysis Processes Through Measurement and Analysis of Textual Information.* www.sei.cmu.edu/pub/documents /08.reports/08tr018.pdf

Andrew P. Moore, Dawn M. Cappelli, & Randall F. Trzeciak. *The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures.* www.sei.cmu.edu/pub/ documents/08.reports/08tr009.pdf

David M. Raffo & Wayne Wakeland. *Moving Up the CMMI Capability and Maturity Levels Using Simulation*. www.sei.cmu.edu /pub/documents/08.reports/08tr002.pdf

Karen Richter. *CMMI for Acquisition (CMMI-ACQ) Primer, Version 1.2*. www.sei.cmu.edu/pub/documents /08.reports/08tr010.pdf

Cal Waits, Joseph Ayo Akinyele, Richard Nolan, & Larry Rogers. *Computer Forensics: Results of Live Response Inquiry vs. Memory Image Analysis*. www.sei.cmu.edu/pub/documents /08.reports/08tn017.pdf

Lutz Wrage, Soumya Simanta, Grace A. Lewis, & Saul Jaspan. *T-Check in Technologies for Interoperability: Web Services and Security—Single Sign-On*. www.sei.cmu.edu/pub/documents /08.reports/08tn026.pdf

Articles

Len Bass, Robert Nord, William Wood, David Zubrow, & Ipek Ozkaya. "Analysis of Architecture Evaluation Data." *Journal of Systems and Software*, September 2008.

Sagar Chaki, Edmund Clarke, Natasha Sharygina, & Nishant Sinha. "Verification of Evolving Software via Component Substitutability Analysis." *Formal Methods in System Design (FMSD)* 32, 3, June 2008: 235-266.

Sagar Chaki & Ofer Strichman. "Three Optimizations for Assume-Guarantee Reasoning with L*." *Formal Methods in System Design (FMSD)* 32, 3, June 2008: 267-284.

Suzanne Garcia (with Sandra Cepeda & Jacquelyn Langhout). "Is CMMI Useful and Usable in Small Settings? One Example." *CrossTalk*, February 2008.

Caroline Graettinger, Suzanne Garcia, William Peterson, Christian Carmody, & M. Lynn Penn. "Field Guide to Provide Step-by-Step Examples for Improving Processes in Small Settings." *CrossTalk*, February 2008.

Watts Humphrey. "The Process Revolution." *CrossTalk*, 2008.

Watts Humphrey. "The Software Quality Challenge." *CrossTalk*, 2008.

Watts Humphrey. "Hindsight, Insight and Foresight from the Greatest Minds: Software Process: Past, Present and Future." *Frontier Journal*, August 2008.

Watts Humphrey (with Dieter Rombach, Jurgen Munch, Alexis Ocampo, & Dan Burton). "Teaching Disciplined Software Development." *The Journal of Systems & Software,* May 2008, 747-763.

Grace Lewis, Soumya Simanta, Edwin Morris, Lutz Wrage, & Dennis Smith. "Common Misconceptions About Service-Oriented Architecture." *CrossTalk*, November 2007.

Nancy Mead (with Jonathan P. Caulkins, Eric Hough, & Hassan Osman). "Optimizing Investments in Security Countermeasures: A Practical Tool for Fixed Budgets." *IEEE Security & Privacy*, September/October 2007.

Nancy R. Mead (with Jeffrey A. Ingalsbe, Louis Kunimatsu,Tim Baeten). "Threat Modeling: Diving into the Deep End." *IEEE Software Special Issue on Software Quality Requirements 25*, 1, January/February 2008: 28-34.

Nancy R. Mead (with Daniel Shoemaker & Jeffrey A. Ingalsbe). "Integrating Software Assurance Knowledge Into Conventional Curricula." *CrossTalk*, January 2008.

Ipek Ozkaya, Len Bass, Robert Nord, & Rajinder S. Sangwan. "Making Practical Use of Quality Attribute Information." *IEEE Software 25*, 2, March-April 2008: 25-33.

Books

Julia H. Allen, Sean Barnum, Robert J. Ellison, Gary McGraw, & Nancy R. Mead. *Software Security Engineering: A Guide for Project Managers*. Upper Saddle River, NJ: Addison-Wesley, 2008 (ISBN: 9780321509178).

Robert C. Seacord. *Secure Coding in C and C++*. Upper Saddle River, NJ: Addison-Wesley, 2005 (ISBN: 0321335724).

Jeannine M. Siviy, M. Lynn Penn, & Robert W. Stoddard. *CMMI and Six Sigma: Partners in Process Improvement*. Upper Saddle River, NJ: Addison-Wesley, 2008 (ISBN: 9780321516084).

Book Chapters

Emmanuel Baker & Matthew J. Fisher. "Organizing for Quality Management," 1-34. *Handbook of Software Quality Assurance*. Boston: Artech House, 2008 (ISBN: 9781596931862).

Emmanuel Baker & Matthew J. Fisher "Training for Quality Management, " 111-119. *Handbook of Software Quality Assurance*. Boston: Artech House, 2008 (ISBN: 9781596931862).

Nancy R. Mead. "Identifying Security Requirements Using the Security Quality Requirements Engineering (SQUARE) Method," 943-963. *Information Security and Ethics: Concepts, Methodologies, Tools and Applications*. Hershey, PA: Idea Group Reference, 2008 (ISBN: 9781599049373).

Keynote Presentations

Palma Buttles-Valdez

"The People CMM as a Contributor to Organizational Success," 3rd Annual Congress of Technology and Information Querétaro, February 2008

"Organizational Culture and People Issues in Process Improvement," CoMMIt Symposium, September 2008

Clyde Chittister (with Bob Rassa)

"CMMI Current State and Future Plans," 7th Annual CMMI Workshop for SCAMPI Lead Appraisers and CMMI Instructors, Denver, CO, November 2007.

Watts S. Humphrey

"Faster, Cheaper, Worse!" World Software Quality Congress, Crystal City, October 2008.

"Software: The Competitive Edge," CIISA Conference, September 2008.

"The Victim Trap," Team Software Process Symposium 2008, September 2008.

"The Victim Trap," European Software Engineering Process Group Conference, June 2008.

"Software: The Competitive Edge," National Encounter PROSOFT 2.0, May 2008.

"Winning Software Teams," Adobe Annual Technology Summit Meeting, February 2008.

"Large Scale Knowledge Work," Software Engineering Process Group Conference, December 2007.

"Large-Scale Knowledge Work," Latin American Software Engineering Process Group Conference, October 2007.

"The Ideal Software Job," ICSPI Conference, October 2007.

"TSP Adoption Issues—Reality or Myth," Software Engineering Process Group Conference, March 2008.

"20 Years of the SEPG: Past Successes, Future Opportunities," Software Engineering Process Group Conference, March 2008.

Mike Konrad

"CMMI and the Future of Systems and Software Engineering," 6th Annual SEPG Australia Conference 2008, August 2008.

Nancy R. Mead

"Software Engineering Education: How Far We've Come and How Far We Have To Go," IEEE Conference on Software Engineering Education & Training (CSEET'08), April 2008.

Paul Nielsen
"Development, Process, and Beyond: A Holistic Approach to Software Engineering," 6th Annual SEPG Australia Conference 2008, August 2008.

Linda Northrop
"Software Product Lines: Today's Impact and Tomorrow's Potential," IBM Future of Software Applications Conference, June 2008, New York.

"Ultra-Large-Scale Systems and the Impact of Scale," 5th International Workshop on Model-Based Methodologies for Pervasive and Embedded Software (part of the ETAPS Conference), March 2008, Budapest, Hungary.

James Smith, II
"Governance for Systems of Systems—Lessons for Global Development?" 46th AIAA Aerospace Sciences Meeting and Exhibit. Reno, January 2008.

"Systems of Systems and Service Oriented Architecture: Opportunities and Challenges," Sixth Earth Science Data Systems Working Group (ESDSWG 2007), October 2007.

Published Proceedings

Richard Baskerville, Linda Levine, Jan Pries-Heje, & Bala Ramesh. "Advances in Information Systems Development: From Discipline and Predictability to Agility and Improvisation." *Proceedings of Advances in Information Systems Research, Education and Practice*. September 7-10, 2008 (Milan, Italy). Springer (0387096817).

Stephany Bellomo & James Smith. "Attributes of Effective Configuration Management For Systems of Systems," 177-184. *Proceedings of the 2nd Annual IEEE International Systems Conference*, April 7-10, 2008 (Montreal, Quebec, Canada).

Stephen Blanchette, Jr. "Military Intervention in Iran: Why and How." *2007 Association of the U.S. Army Annual Meeting and Exposition*, October 8-10, 2007 (Washington, DC).

John Hudak, Lutz Wrage, Jörgen Hansson. "Analyzable Architectural Models of Service-Based Embedded Systems." *Proceedings of the IEEE International Conference on Dependable Systems and Networks*. June 24-27, 2008 (Anchorage, Alaska).

Watts S. Humphrey. "Preparing Students for Industry's Software Engineering Needs," 327-332. *Proceedings of the SIGCSE 2008 Technical Symposium on Computer Science Education.* (Portland, OR).

Linda Levine & William Novak. "Identifying Acquisition Patterns of Failure Using System Archetypes," 327-332. *Proceedings of the 2nd Annual IEEE International Systems Conference*, April 7-10, 2007 (Montreal, Canada). Piscataway, NJ: IEEE Computer Society.

James McCurley. "Measurement Experiences with Six Sigma," *Proceedings of the 12th Annual PSM Users' Group Conference Improving Organizational Performance through Measurement Insight*, July 14-18, 2008 (Mystic, Connecticut).

Nancy R. Mead. "Software Engineering Education: How Far We've Come and How Far We Have To Go," 18-22. *IEEE Conference on Software Engineering Education & Training* (CSEET'08), April 15-17, 2008 (Charleston, SC). IEEE Computer Society.

Nancy R. Mead (with Dan Shoemaker, Antonio Drommi, & Jeff Ingalsbe). "Immersion Program to Help Students Understand the Impact of Cross Cultural Differences in Software Engineering Work," 455-459. *COMPSAC (International Computer Software and Applications Conference)*. July 28 - August 1, 2008 (Turku, Finland). IEEE Computer Society.

Nancy R. Mead (with Dan Shoemaker, Antonio Drommi, & Jeff Ingalsbe). "Integrating Secure Software Assurance Content with SE2004 Recommendations," 59-66. *21st Conference on Software Engineering Education & Training*, April 15-17, 2008. IEEE Computer Society.

Nancy R. Mead, Venkatesh Viswanathan, & Deepa Padmanabhan. "Incorporating Security Requirements Engineering into the Dynamic Systems Development Method," 949-954. *Proceedings of the COMPSAC (International Computer Software and Applications Conference) 2008, IWSSE Workshop (International Workshop on Security and Software Engineering)*. July 28, 2008 (Turku, Finland). IEEE Computer Society.

Nancy R. Mead, Venkatesh Viswanathan, & Justin Zhan. "Incorporating Security Requirements Engineering into the Rational Unified Process," 537- 542. *Proceedings of the 2008 International Conference on Information Security and Assurance (ISA)*. April 26-28, 2008 (Busan, Korea). IEEE Computer Society.

James McCurley. "Goal-Driven Measurement", *U.S. Census Bureau Software Process Improvement Conference*, September 2008.

Carol Sledge, Daniel Manson, Anna Maria Berta, Dena Haritos Tsamitis. "Five Years of Success: Some Outcomes of the Carnegie Mellon Information Assurance Capacity Building Program." *Proceedings of the 2007 ISECON (Information Systems Education)*, November 1-4, 2007. Pittsburgh, PA.

James Smith & Craig Meyers. "The Programmatics of Acquisition in Systems of Systems," 469-474. In *Proceedings of the 2nd Annual IEEE International Systems Conference*, April 7-10, 2008. Montreal, Quebec, Canada.

Robert Stoddard. "CMMI Process Performance Baselines and Models: Experience and Results," *NDIA CMMI Technology Conference*, November 2007.

Opportunities

Work with the SEI

Congress established the SEI in 1984 because software is vital to the national interest. By working with the SEI, organizations benefit from more than two decades of government investment and participation from organizations worldwide in advancing the practice of software engineering.

The SEI creates, tests, refines, and disseminates a broad range of technologies and management techniques. These techniques enable organizations to improve the results of software projects, the quality and behavior of software systems, and the security and survivability of networked systems.

As an applied research and development center, the SEI brings immediate benefits to its research partners and long-term benefits to organizations that depend on software. The tools and methods developed by the SEI and its research partners are applied daily in organizations throughout the world.

How the SEI Works with Government and Industry

SEI staff members help the U.S. Department of Defense (DoD) and other government agencies solve software engineering and acquisition problems. SEI direct support is funded through task orders for government work. Engagements with the SEI are of particular benefit to government program managers, program executive officers, and senior acquisition executives, particularly those with long-range programs that will benefit from strategic improvements that the SEI fosters.

The SEI has a well-established process for contracting with government agencies and will work with an organization to meet its needs. This process is described in more detail at www.sei.cmu.edu/collaborating/contracting.html.

The SEI works with commercial organizations that want to develop a strategic advantage by rapidly applying improved software engineering technology. The SEI works with organizations that want to combine their expertise with the SEI's expertise to mature new technology for the benefit of the entire software industry. The SEI also supports a select group called SEI Partners, which are organizations and individuals that are trained and licensed by the SEI to deliver SEI products and services.

To determine how to put the SEI to work for your organization, contact SEI Customer Relations at customer-relations@sei.cmu.edu.

SEI Solutions Guide

The SEI Solutions Guide is a summary of the SEI's tools and methods, services, courses, conferences, credentials, books, and opportunities to collaborate with the SEI on research. To receive a copy of the Guide, please contact

Customer Relations
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
1-888-201-4479 or +1 412 268-5800
customer-relations@sei.cmu.edu

See the Solutions Guide online at www.sei.cmu.edu/solutions

SEI Employment

The SEI seeks candidates for its technical, business, and administrative staff divisions. Contact the SEI Human Resources department to learn the benefits of working at the SEI: www.sei.cmu.edu/about/employment.

Copyrights

Trademarks and Service Marks

The SEI Year in Review is produced by SEI Marketing

Manager, Marketing
Janet Rex

Public Relations
Kelly Kimberland, APR

Editor-in-Chief
Richard Lynch

Editorial
Heidi Brayer
Pamela Curtis
Claire Dixon
Ed Desautels
Jennifer Kent
Kelly Kimberland
Richard Lynch
William McSteen
Jerry Miller
John Morley
Amanda Parente
Shilo Raube
Pennie Walters
Barbara White

Design
Cat Zaccardi

Digital Production
Melissa Neely

Image Specialist
Kurt Hess

Photography
Tim Kaulen, Photography and Graphic Services, Mellon Institute

Production
David Gregg
Jeff Balmert

Web Design
Sharon West

Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-2612
Phone: 412-268-5800
Toll-free: 1-888-201-4479
Fax: 412-268-6257
www.sei.cmu.edu
customer-relations@sei.cmu.edu

SEI Colorado Springs
Suite 111
1155 Kelly Johnson Boulevard
Colorado Springs, CO 80920

SEI Europe
An der Welle 4
Reception Level 1
60 322 Frankfurt
Germany

SEI Washington, DC
NRECA Building
Suite 200
4301 Wilson Boulevard
Arlington, VA 22203